


# 7 / 8WAN VPN 防火墙

具负载平衡，带宽管理，VPN 与网络安全等功能

简体中文使用手册

www.Qno.cn

# 产品功能说明手册使用许可协议

《产品功能说明手册（以下称”手册”）使用许可协议》（以下称”协议”）是用户与侠诺科技股份有限公司（以下称”侠诺”）关于手册许可使用及相关方面的权利义务、以及免除或者限制侠诺责任的免责条款。直接或间接取得本手册档案以及享有相关服务的用户，都必须遵守此协议。

重要须知：侠诺在此提醒用户在下载、阅读手册前阅读本《协议》中各条款。请您审阅并选择接受或不接受本《协议》。除非您接受本《协议》条款，否则请您退回本手册及其相关服务。您的下载、阅读等使用行为将视为对本《协议》的接受，并同意接受本《协议》各项条款的约束。

【1】知识产权声明
手册内任何文字表述及其组合、图标、界面设计、印刷材料、或电子文件等均受我国著作权法和国际著作权条约以及其它知识产权法律法规的保护。当用户复制"手册"时，也必须复制并标示此知识产权声明。否则，侠诺视其为侵权行为，将适时予以依法追究。

【2】"手册"授权范围：
用户可以在配套使用的计算机上安装、使用、显示、阅读本"手册"。

【3】用户使用须知
用户在遵守法律及本协议的前提下可依本《协议》使用本"手册"。用户若是违反本《协议》，侠诺将中止其使用权力并立即销毁此"手册"的复本。本手册"纸质或电子档案"，仅限于为信息和非商业或个人之目的使用，并且不得在任何网络计算机上复制或公布，也不得在任何媒体上传播;及不得对任何"档案"作任何修改。为任何其它目的之使用,均被法律明确禁止,并可导致严重的民事及刑事处罚。违反者将在可能的最大程度上受到指控。

【4】法律责任与免责声明
【4-1】侠诺将全力检查文字及图片中的错误，但对于可能出现的疏漏，用户或相关人士因此而遭受的直接或间接的经济损失、数据损毁或其它连带的商业损失，侠诺及其经销商与供货商不承担任何责任。
【4-2】侠诺为了保障公司业务发展和调整的自主权，侠诺拥有随时自行修改或中断软件 / 手册授权而不需通知用户的权利，产品升级或技术规格如有变化，恕不另行通知，如有必要，修改或中断会以通告形式公布于侠诺网站的相关版块。
【4-3】所有设置参数均为范例，仅供参考，您也可以对本手册提出意见或建议，我们会参考并在下一版本作出修正。
【4-4】本手册为解说同系列产品所有的功能设置方式，产品功能会按实际机种型号不同而有部份差异，因此部分功能可能不会出现在您所购买的产品上。





【4-5】侠诺保留此手册档案内容的修改权利，并且可能不会实时更新手册内容，欲进一步了解产品相关更新讯息，请至侠诺官方网站浏览。

【4-6】侠诺（和/或）其各供货商特此声明，对所有与该信息有关的保证和条件不负任何责任，该保证和条件包括关于适销性、符合特定用途、所有权和非侵权的所有默示保证和条件。所提到的真实公司和产品的名称可能是其各自所有者的商标，侠诺（和/或）其各供货商不提供其它公司之产品或软件等。在任何情况下,在由于使用或档案上的信息所引起的或与该使用或运行有关的诉讼中，侠诺和/或其各供货商就因丧失使用、数据或利润所导致的任何特别的、间接的或衍生性的损失或任何种类的损失，均不负任何责任，无论该诉讼是合同之诉、疏忽或其它侵权行为之诉。

【5】其它条款

【5-1】本协议高于任何其它口头的说明或书面纪录，所定的任何条款的部分或全部无效者，不影响其它条款的效力。

【5-2】本协议的解释、效力及纠纷的解决，适用于台湾法律。若用户和侠诺之间发生任何纠纷或争议，首先应友好协商解决。若协商未果，用户在完全同意将纠纷或争议提交侠诺所在地法院管辖。中国则以「中国国际经济贸易仲裁委员会」为仲裁机构。





# 目 录







一、簡介

7 / 8 WAN VPN 防火墙，是一台符合中大型企业，网吧及社区等的 Multi-WAN 旗舰型机种，高效能整合新一代设计的多 WAN 口防火墙。它除了具备绝大多数宽带市场适用的对外联机能力外，还内建了 10/100Mbps QoS 及 VLAN 交换机，以满足多数企业、网吧对防火墙的市场需求。

它内建了数个 10/100 Base-T/TX 以太网(RJ45) 广域网端口。这些广域网端口不仅可以支持高效能网络智能负载均衡模式，指定路由，并且还支持策略路由提供弹性灵活的网络需求设置，同时还支持 DHCP、固定 IP、PPPoE、桥接模式、VPN 透通、端口绑定、静态路由、动态路由、NAT、一对一 NAT、PAT、MAC Clone、支持动态域名解析。LAN 口方面也内建了数个 10/100 Base-T/TX 以太网(RJ45)以及 1 个 DMZ 10/100 Base-T/TX 以太网(RJ45)端口。支持虚拟主机功能、微软 UPnP 功能、VLAN、多网域(Multi Subnet)以及公网 IP 透通模式，内网使用公网 IP 地址运作无障碍。

配合新一代、多样化、高安全整合性的防火墙设备需求环境，内建超高速 Intel IXP425 533MHz 高效能四核心处理器，在高速处理架构下，发挥超高的网络效能。处理速度及带机量直逼中、大型企业用户专用的昂贵 VPN 防火墙设备；并获得企业界广泛的应用系统支持。

除了宽带市场适用的对外联机能力外，它还具备 VPN 虚拟网络联机功能，目前企业广泛应用的虚拟私有网络硬件加速模式，提供完整 VPN 功能。

Qno 支持标准的 IPSec 协议，IPSec VPN 支持 DES、3DES、AES-128 加密，MD5、SH1 认证，IKE Pre-Share Key、或是手动设置的密钥交换。支持野蛮模式，断线后自动重新联机，以及网上邻居透通。支持群组式浮动 IP 客户端与总部进行虚拟私有网联机。

具备 PPTP 服务器功能，具备联机状态显示。每个 WAN 口可同时建立多种 DDNS 设置，可使用动态 IP 建立 VPN 联机。VPN 防火墙

支持 VPN 备援功能，断线可从另一个 WAN 自动建立 VPN 联机，每个 WAN 口可同时建立多种 DDNS 设置，可使用动态 IP 建立 VPN 联机。支持 VPN 备援功能，断线可从另一个 WAN 自动建立 VPN 联机。

VPN 方面独有 QVM VPN－SmartLink IPSec VPN 设置，只需输入 VPN 服务器 IP、用户名、密码即可自动完成 IPSec VPN 建置，进入 VPN 防火墙领先同行且是 Qno 独创的 QVM 功能，可设置为 QVM 服务器功能接受客户端其它 QVM 系列产品建立虚拟私有网联机，让用户简易完成 VPN 设置，无需网管也能办到，让企业享有 VPN 的优点，而不必顾虑技术及管理上的困难。中央控制的功能，可以随时通过此功能远程登录到客户端进行中央控管，安全及保密性绝对符合 IPSec 理念及规范。支持备援功能，断线可从另一个 WAN 自动建立联机，确保 VPN 服务永不断线。

VPN 防火墙内建进阶型防火墙功能，能够阻绝大多数的网络攻击行为，使用了 SPI 数据包主动侦测检验技术(Stateful Packet Inspection)，数据包检验型防火墙主要运作在网络层，执行对每个连接的动态检验，也拥有应用程序的警示功能，让数据包检验型防火墙可以拒绝非标准的通讯协议所使用的连接，





默认自动侦测并阻挡。VPN 防火墙亦同时支持使用网络地址转换 NA 功能以及路由模式，使网络环境架构更为弹性，易于规划管理。

通过网页内容管制设置，允许企业内部自定网络存取规则，管理页面内建可新增移除的过滤名单，可让用户选择应该禁止存取或记录监控哪些种类的网站，如此可对学校或企业的 Internet 管理有明确的作用，设置过滤设置并通过完整的 OS 管理核心进行管理。VPN 防火墙提供线上多样化的日志(SysLog)记录，支持线上管理设置工具，可清楚易懂的知道网络设置状态、并加强管理全部的网络安全存取规则、VPN、及其它服务等。

VPN 防火墙能充分保障各种分支机构办公室及各点间通讯的安全，避免日益趋多的商业机密窃取与攻击破坏等。专属的 OS 独立式作业平台，使用者无须具备专业级的网络知识即可安装使用。通过浏览器如:IE，Netscape...来设置与管理 VPN 防火墙。





## 二、多 WAN VPN 防火墙设置操作流程

本章节介绍用户整体设置多 WAN VPN 防火墙操作流程，通过对 VPN 防火墙多 WAN 设置流程的了解可以很轻松的设置我们的网络，来有效的管理我们的网络，使 VPN 防火墙达到应有的功能，使 VPN 防火墙的效能达到最高。

### 2.1 系统性设置流程的需要

用户可以通过以下操作流程设置网络，能够使网络有效利用带宽，网络效能达到理想的效果，同时可以阻断一些攻击与预防一些安全隐患，通过流程设置更加方便用户的安装与操作，简化维护管理的难度，使得用户的网络设置一次到位。设置主要流程如下：

1、 硬件安装。

2、 登录设置窗口。

3、 确定设备规格及进行密码和时间设置。

4、 进行广域网联机的设置：进行内部联机的设置。

5、 进行局域网联机的设置：实体线路设置及 IP 地址设置

6、 进行 QoS 带宽管理设置：防止带宽占用情况。

7、 进行防火墙设置：预防攻击及不当存取网络资源。

8、 其它特别设置：开放服务器、UPnP、DDNS、MAC Clone。

9、 管理维护的设置系统日志、SNMP、及设置参数备份注销设置窗口。

10、VPN 虚拟专用网、QnoKey、QVM VPN 功能设置

11、注销设置窗口

### 2.2 设置流程表

下表主要阐述每个设置流程相对应的 VPN 防火墙管理内容以及此设置所达到的目的，如需详细了解每步过程以及后面章节介绍所对应的内容，可参考（附录一、设置界面及使用手册章节对照）。

| # | 设置 | 内容 | 目的 |
|---|---|---|---|
| 1 | 硬件安装 | 构建用户需要的网络 | 根据用户实地网络的要求来安 VPN 防火墙硬件。 |





| 2 | 登录设置窗口 | 从计算器 Web 接入 VPN 防火墙设置窗口，了解系统信息 | 登录 VPN 防火墙的 Web 管理页面。 |
|---|---|---|---|
| 3 | 确定设备规格 | 确定产品软件版本以及路由工作情况 | 确定 VPN 防火墙规格，系统软件版本，以及 VPN 防火墙工作状况。 |
| | 进行密码及时间设置 | 设置时间及修改密码 | 安全的考虑修改登录密码。<br>设置 VPN 防火墙时间与广域网络同步。 |
| 4 | 进行广域网联机的设置 | 确定广域网线路设置、带宽调配、及协议绑定 | 连接广域网络，通过带宽的设置等能更好的利用带宽，优化数据转发能力。 |
| 5 | 进行局域网联机的设置：实体线路设置及 IP 地址设置 | 端口镜像及 VLAN 设置。内部用户 IP 的分配群组及管理 | 应地区需求提供端口镜像功能，同时改进端口管理及 VLAN 的设置满足内网相关需求，弹性提供固定 IP/DHCP 自动 IP 地址分配，方便用户在不同网络环境的需要。IP 群组管理对一组 IP 地址做相同设置，简化管理工作。 |
| 6 | 进行 QoS 带宽管理设置，防止带宽占用情况的发生 | 广域网端口、内部用户或应用流量及联机数的限制 | 确保网络重要信息不致延迟、确保网络重要应用服务联机顺畅；进一步针对现有的带宽进行管理运用，让有限的带宽资源发挥最大的效用。 |
| 7 | 进行防火墙设置，预防攻击及非法访问网络资源 | 攻击阻挡、访问规则及网页存取限制 | 当内网用户使用 BT、点点通影响其它人上网、员工上班时间不正当上网以及使用 MSN、QQ、Skype 影响工作效率；当网速因被黑客攻击而受影响或内网用户常被蠕虫及 ARP 软件所苦；网管可依据需求设置内外网络存取规则，以进一步管控员工个别上网行为。 |
| 8 | 其它特别设置：开放服务器、UPnP、DDNS、MAC Clone | 针对内部设置开放服务器、UPnP、路由模式、多广域网 IP、DDNS、Mac 克隆 | 高级管理设置完成对网络的更高一步要求，构建内部开放服务器，虚拟服务器，UPnP 通讯协议的设置，设置动态路由或者静态路由，一对一 NAT 设置，动态域名解析服务与 Mac 地址克隆。 |
| 9 | 管理维护的设置：系统日志、SNMP、及设置参数备份 | VPN 防火墙工作情况监测、系统参数的备份 | 网管可借此功能查看系统日志、即时监控系统状态及内外流量，确保内网运作无误。 |
| 10 | VPN 虚拟专用网、QnoKey、QVM VPN 功能设置 | 针对 VPN 联机功能进行设置，包括 PPTP、QnoKey 与 QVM VPN | 借由多种而简便的 VPN 设置，使各类的 VPN 虚拟专用网应用环境，能有效并顺利地运作 |





| 11 | 注销设置窗口 | 离开设置窗口 | 注销退出 VPN 防火墙 Web 管理页面。 |
|---|---|---|---|

下面我们就根据这个流程来设置完成我们的网络设置。





三、硬件安装

本章介绍产品的硬件接口以及实体安装。

3.1 VPN 防火墙 LED 显示灯

LED 灯号说明

| LED | 颜色 | 意义 |
|---|---|---|
| Power-电源 | 绿灯 | 绿灯亮： 电源开启连接 |
| DIAG-自我测试 | 橘灯 | 橘灯亮： 系统尚未完成开机自我检测功能。<br>橘灯熄灭： 系统已经正常完成开机自我检测功能。 |
| Link/Act-联机/动作<br>（端口右侧绿灯） | 绿灯 | 绿灯亮： 以太网络联机正常<br>绿灯闪烁： 以太网络端口正在传送/接收数据包数据传输 |
| 100M-速度<br>（端口左侧橘黄灯） | 橘灯 | 橘灯亮： 以太网络联机在 100Mbps 的速度<br>橘灯熄灭： 以太网络联机在 10Mbps 的速度 |
| Connect-互联网 | 绿灯 | 绿灯亮： 广域端口已经联机并取得 IP 地址 |

硬件恢复（Reset）按键

| 动作 | 意义 |
|---|---|
| 点击 Reset 按钮 5 秒 | 热开机，重新启动 VPN 防火墙<br>DIAG 灯号： 橘色灯号慢慢闪烁 |
| 点击 Reset 按钮 10 秒以上 | 恢复原出厂默认值<br>DIAG 灯号： 橘色灯号快闪 |

系统内建电池

VPN 防火墙内建有系统时间的电池，此电池的寿命约为 1～2 年，当电池已经无法充电或是使用寿命到达后，VPN 防火墙将无法记录时间或是连接互联网同步 NTP 时间服务器。您必须与您的供应商联系，以便取得更换电池技术。

注意！

为了产品的正常运行，请勿自行更换电池，以免造成产品无法恢复的损坏！

将 VPN 防火墙安装在 19"标准机架上

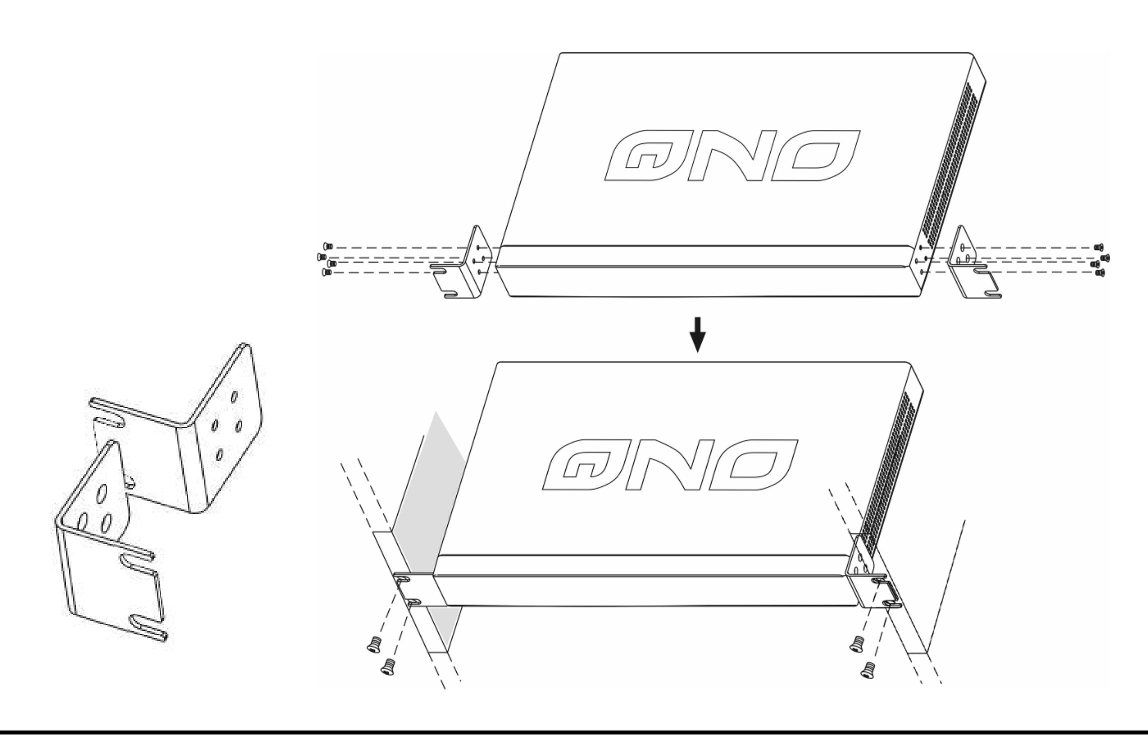
建议您可以将 VPN 防火墙放置于桌上使用，或是您有机房专用 19 吋标准机架的话，可以将 VPN 防火墙安装于机架上，每一台 VPN 防火墙都有配备专用连接机架配件。当您安装 VPN 防火墙于机架上的时候，请注





意不要将其它过重的物品堆栈或是放置于机器上，以免因无法负重而发生危险或是损伤机器本体。

每一台 VPN 防火墙都有配备专用连接机架配件，包含 2 只 L 型锁附架以及八颗专用螺丝，用来将 VPN 防火墙安装在机架上使用。安装于您的 19 吋标准机架上的方法如下图所示：



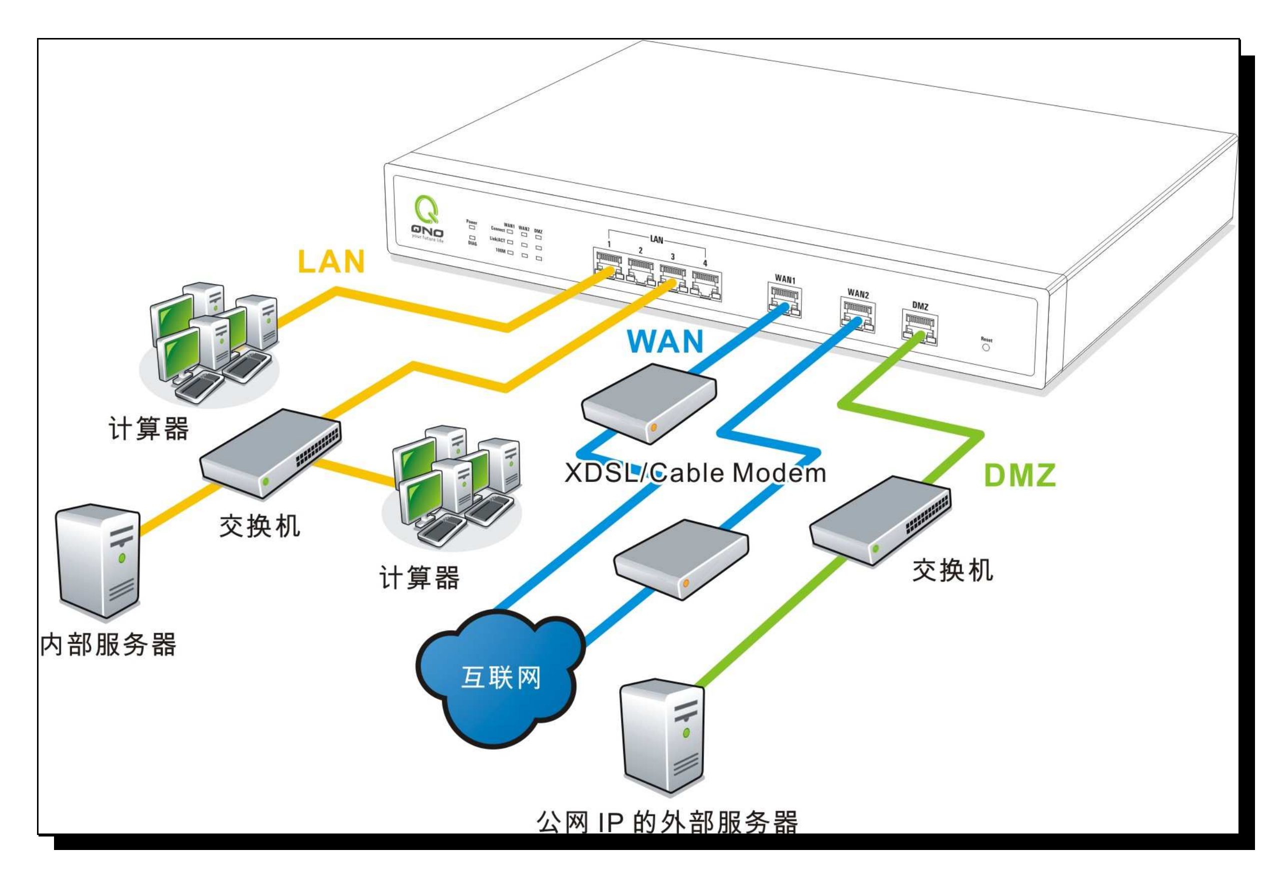
注意！

为了产品的稳定运行，无论您是如何放置 VPN 防火墙，请不要阻塞产品两侧通风口的任何一侧，并保持通风口有 10 厘米以上的通风空间！






## 3.2 VPN 防火墙的网络连接




广域网络联机：连接 xDSL Modem 或光纤盒来连通互联网。或是连接交换机或外部路由器、防火墙来连通您现有的网络。

局域网络联机：连接交换机或计算机。若局域网端口有支持镜像功能，请在“端口管理”中做设置，设定完成即可直接将监控或过滤服务器接在此端口使用

DMZ 端口：此端口可以连接如 Switch HUB 或是具有外部合法 IP 地址的服务器，如网页服务器以及电子邮件服务器等。





四、登录 VPN 防火墙

本章主要是在客户连接好 VPN 防火墙后 通过连接 VPN 防火墙的计算机登录 VPN 防火墙的 Web 管理页。

首先在连接到 VPN 防火墙 LAN 端的计算机（确定计算机是自动获得 IP 地址）上的 DOS 下查找 VPN 防火墙的 IP 地址，点开始→运行，输入“cmd”命令进入 DOS 操作，再输入“ipconfig”命令→确认，查到默认网关（Default Gateway）地址如图，192.168.1.1。确认默认网关也就是 VPN 防火墙的默认 IP 地址。

```
C:\WINDOWS\system32\CMD.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\PM01>ipconfig

Windows IP Configuration


Ethernet adapter 區域連線:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\PM01>_
```

注意！

当“ipconfig”不能获得 IP 地址以及默认网关的情况，或者获得的 IP 地址为 0.0.0.0 以及 169.X.X.X 的情况，就是 VPN 防火墙并没有分配到 IP 地址，建议用户检查线路是否有问题，计算机网卡是否接好等。






然后开启网页浏览器（如 IE），在网址栏输入 192.168.1.1（VPN 防火墙的默认网关），会出现以下的登录窗口：




VPN 防火墙默认的使用者名称(User Name)与使用者密码(Password)皆为"admin"，您可以在进入路由管理页面后）更改此用户名及登录密码。

注意！

为了安全，我们强烈建议您务必在登录之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录至 VPN 防火墙的设置窗口，必须点击面板上的 Reset 按键十秒以上，恢复到出厂值，其所有设置将需要重新设置。

登录后，就会显示 VPN 防火墙的 Web 管理页面，在其页面的右上角选择 VPN 防火墙操作的语言模式，选中的图标将变成蓝色，这里选择"简体"（简体中文版本），如图。



五、确定设备规格、状态显示以及登录密码和时间的设置

本章介绍登录软件设置窗口后，进入首页可以了解到的设备规格以及设备工作状态信息，还有因安全考虑需要用户即时修改登录密码与系统时间设置。

## 5.1 首页显示

首页显示 VPN 防火墙目前系统所有参数以及状态显示信息。

### 5.1.1 系统信息

**广域网状态**

| 接口位置 | 广域网1 | 广域网2 | 广域网3 | 广域网4 | DMZ |
|---|---|---|---|---|---|
| IP地址 | 0.0.0.0 | 220.130.188.40 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| 默认网关 | 0.0.0.0 | 220.130.188.33 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| DNS 服务器 | 0.0.0.0 | 168.95.1.1<br>0.0.0.0 | 0.0.0.0 | 0.0.0.0 | --- |
| 会话数 | 0 | 3 | 0 | 0 | 0 |
| 下载带宽使用率(%) | 0 | 0 | 0 | 0 | |
| 上传带宽使用率(%) | 0 | 0 | 0 | 0 | |
| 动态域名服務 | Dyndns 关闭<br>3322 关闭<br>Dtdns 关闭<br>Qnoddns 关闭 | Dyndns 关闭<br>3322 关闭<br>Dtdns 关闭<br>Qnoddns 关闭 | Dyndns 关闭<br>3322 关闭<br>Dtdns 关闭<br>Qnoddns 关闭 | Dyndns 关闭<br>3322 关闭<br>Dtdns 关闭<br>Qnoddns 关闭 | --- |
| QoS带宽管理 | 0 条规则 | 0 条规则 | 0 条规则 | 0 条规则 | --- |
| 手动连接 | 释放<br>更新 | | 释放<br>更新 | 释放<br>更新 | --- |

IP 地址： 此为显示 VPN 防火墙 WAN 端目前的 IP 地址信息。
默认网关： 此为显示 ISP 分配给 VPN 防火墙 WAN 的网关 IP 地址信息。
DNS 服务器： 此为显示 VPN 防火墙的 DNS 的 IP 地址信息。
会话数： 此为显示 VPN 防火墙每个 WAN 目前的会话数目。
下载带宽使用率： 此为显示 VPN 防火墙每个 WAN 目前的下载带宽使用比例。
上传带宽使用率： 此为显示 VPN 防火墙每个 WAN 目前的上传带宽使用比例。
动态域名服务： 此为显示 VPN 防火墙的 DDNS 是否启动的状态信息。系统默认此功能为关闭。
QoS 带宽管理： 此为显示 VPN 防火墙的网络质量服务(QoS)是否开启。
手动连接： 当使用者选择自动取得 IP 地址时，他会显示二个按钮分别为释放与更新。使用者可以点击释放按钮去做释放 ISP 端所核发的 IP 地址，以及点击更新按钮去做更新 ISP 端所核发的 IP 地址。

|  | 当选择 WAN 端联机使用如 PPPoE 或是 PPTP 的话 它会变为显示"连接"与"中断"。 |
|---|---|
| DMZ IP 地址： | 此为显示 VPN 防火墙 DMZ 目前的 IP 地址设置信息。 |

5.1.2 硬件端口状态实时显示

**端口配置状态**

| 端口号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 接口位置 | 局域网 | | | | | | | |
| 状态 | 激活 | 激活 | 激活 | 激活 | 激活 | 激活 | 激活 | 激活 |

| 端口号 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | DMZ |
|---|---|---|---|---|---|---|---|---|
| 接口位置 | 局域网 | | | 广域网4 | 广域网3 | 广域网2 | 广域网1 | DMZ |
| 状态 | 激活 | 激活 | 激活 | 激活 | 激活 | 连接 | 激活 | 激活 |

此窗口会显示系统各端口目前实时状态：(连接-已经连接，激活-此端口处于开启状态，关闭-此端口处于关闭状态)。您可以点击此状态按钮，在弹出的窗口中查看各端口更详细的资料显示。如下图：

广域网2 信息

**摘要信息：**

| | |
|---|---|
| 网路连接状态 | 10Base-T / 100Base-TX |
| 接口位置 | 广域网2 |
| 线路连线状态 | 激活 |
| 端口配置状态 | 端口激活 |
| 优先级设定 | 一般 |
| 连接速率 | 100 Mbps |
| 半双/全双工模式 | 全双工 |
| 自动翻转功能 | 激活 |

**流量实时状态：**

| | |
|---|---|
| 接收数据包统计 | 0 |
| 数据包接收Byte数量 | 107885800 |
| 传送数据包统计 | 0 |
| 数据包传送Byte数量 | 65509869 |
| 错误数据包统计 | 0 |

刷新 关闭

此表会显示目前该端口设置状态，如网路连接状态(10Base-T/100Base-TX/1000Base-T)，接口位置(广域网／局域网/DMZ)，线路连接状态(激活/关闭)，端口设置状态(端口激活/端口关闭)，优先级设置(高级/一般)，网络连接速率(10Mbps/100Mbps)，工作模式(半双工/全双工)，以太网自动翻转功能(激活/关闭)。于此项目表格中，会显示此端口的接收和传送的数据包以及数据包传送 Byte 数及数据包错误率等并计算总数量。

### 5.1.3 系统信息

**系统信息**

| | |
|---|---|
| 局域网网关/子网掩码 | 10.10.10.1/255.255.255.0 |
| 工作模式 | NAT模式 |
| 运作时间 | 7天 7时 10分 25秒 |

| | |
|---|---|
| 序列号 | |
| 软件版本 | 2.1.0.1-Qno (Jun 26 2008 20:38:08) |
| 当前时间 | Fri Jul 4 2008 18:21:06 |

局域网网关地址： 此为显示 VPN 防火墙 P 本身的 LAN 端目前 IP 地址，系统默认为 192.168.1.1。

工作模式： 此为显示 VPN 防火墙的目前工作模式(可为 NAT 模式或是路由模式)。

系统默认此功能为 NAT 模式。

运作时间：此为显示 VPN 防火墙目前已经开机的时间。

主机序列号：此为显示 VPN 防火墙的产品序号。

软件版本： 此为显示 VPN 防火墙 目前使用的硬件版本。

当前时间：此显示 VPN 防火墙 目前正确时间，但必须注意，您需要正确设置与远程 NTP 服务器的时间同步后才会正确显示。

## 5.1.4 防火墙状态

**防火墙状态**

| 防火墙 | 状态 |
|---|---|
| SPI数据包检测 | 激活 |
| 防止DoS攻击功能 | 激活 |
| 阻止广域网回应功能 | 关闭 |
| 防止ARP病毒攻击 | 关闭 |
| 远程管理功能 | 激活 |
| 访问规则设置 | 7 条规则 |

SPI 数据包检测：此为显示 VPN 防火墙的 SPI 主动数据包侦测过滤功能选项是否激活(激活/关闭)。

系统默认此功能为激活。

防止 DoS 攻击功能：此为显示 VPN 防火墙的阻断来自网络上的 DoS 攻击功能选项是否开启(激活/关闭)。

系统默认此功能为激活。

阻止广域网回应功能：此为显示 VPN 防火墙的阻断来自网络上的 ICMP-Ping 的响应功能选项是否激活(激活/关闭)。系统默认此功能为激活。

防止 ARP 病毒攻击：此为显示 VPN 防火墙防止 ARP 攻击的功能选项是否激活(激活/关闭)。

系统默认此功能为关闭。

远程管理功能：此为显示 VPN 防火墙的远程管理功能选项是否启动(激活/关闭)。系统默认此功能为关闭。

访问规则设置： 此为显示 VPN 防火墙的访问规则设置的数目。

5.1.5 VPN 虚拟专用网状态

VPN虚拟专用网状态

| VPN配置 | 状态 |
| --- | --- |
| 已使用的隧道数目 | 0 |
| 可使用的隧道数目 | 150 |
| PPTP服务器 | 关闭 |

VPN 设置状态: 此为显示 VPN 防火墙的 VPN 功能选项内容信息。

已使用的隧道数目:此为显示 VPN 防火墙的 VPN 功能目前已经设置的隧道数量。

可使用的隧道数目：此为显示 VPN 防火墙的 VPN 功能目前可使用的隧道数量。

PPTP 服务器：显示 PPTP 服务器是否开启。

5.1.6 系统日志设置状态显示

系统日志配置状态

| 发送到日志服务器 | 关闭 |
| --- | --- |
| 发送到电子邮箱 | 关闭 |

发送到日志服务器： 此为显示您所设置 VPN 防火墙日志记录接收的服务器。

发送到电子邮箱： 此为显示您所设置的 E-mail 地址，VPN 防火墙的日志记录经由此 E-mail 传送出去。

电子邮箱的链接将会连到系统日志设置窗口中：

1. 若您没有设置电子邮件服务器于系统日志设置中，将显示〝邮件无法传送,因为没有设置 SMTP 服务器正确地址”——表示您没设置电子邮件服务器所以无法发送系统日志电子邮件。

2. 若您已经设置电子邮件服务器于系统日志设置中，但是日志尚未达到设置传送的条件时,将显示〝邮件设置已经设置”——表示您的电子邮件服务器已经设置，但是日志尚未达到设置传送的条件时。

3. 若您已经设置电子邮件服务器于系统日志设置中，日志也已经传送出去时，它将显示〝邮件设置已经设置并正常发送”——表示您的电子邮件服务器已经设置，并且已经发送。





4. 若您已经设置电子邮件服务器于系统日志设置中， 但是日志无法正确传送出去时，它将显示〝邮件不能发送，请使用正确的设置"——电子邮件服务器已经设置，但是无法传送出去，可能是设置有问题。





## 5.2 登录密码及时间的修改和设置

### 5.2.1 密码设置

当您每次登录 VPN 防火墙的设置窗口时，必须输入密码，VPN 防火墙的用户名和密码出厂值均为"admin"。考虑安全因素，我们强烈建议您务必在第一次登录并完成设置之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录 VPN 防火墙的设置窗口，必须点击 VPN 防火墙前面板上的 Reset 按键十秒以上，恢复到出厂值，所有设置值将需要重新设置。

**密码设置**

| | |
|---|---|
| 用户名： | admin |
| 密码： | |
| 更改用户名： | admin |
| 输入新密码： | |
| 再次输入新密码： | |

确定 取消

| | |
|---|---|
| 用户名： | 出厂初始值默认为 admin。 |
| 密码： | 填写原本旧密码（出厂初始值默认为"admin"）。 |
| 更改用户名： | 输入新用户名，如 Qno。 |
| 输入新密码： | 填写要更改的新密码。 |
| 再次输入新密码： | 再次填写更改的新密码以确认。 |
| 确定： | 点击此按钮"确定"存储刚才所修改设置的内容参数。 |
| 取消： | 点击此按钮"取消"清除刚才所修改设置的内容参数，此操作必须于"确定" 存储动作之前才会有效。 |

### 5.2.2 系统时间设置

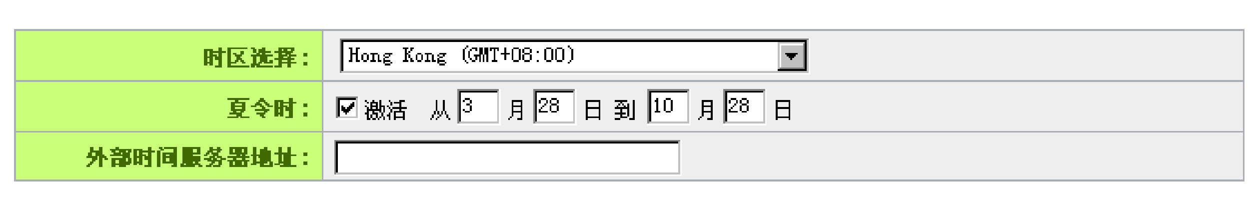
VPN 防火墙可以设置时间，让您在查看 VPN 防火墙的系统纪录或设置网络存取的时间设置时，可以了解事件发生的正确时间，以及作为关闭存取或是开放存取网络资源的依据条件。您可以选择与 VPN 防火墙内建的外部时间服务器(NTP 服务器)取得时间同步，或自己设置正确时间参数。






与外部时间服务器同步：VPN 防火墙有内建的网络时间服务器，会自动同步时间。

◉ **与外部时间服务器同步**
○ **手动配置时间**




确定 取消

| | |
|---|---|
| 时区选择： | 点开下拉菜单选择您所在地点的时区以正确显示当地时间。 |
| 夏令时： | 若是您所的地区有实施日光节约时间，可以输入实施的日期范围，VPN 防火墙会在此日期范围自动调整时间。 |
| 外部时间服务器地址： | 若是您自己有偏爱使用的时间服务器，可以输入该服务器的地址。 |
| 确定： | 点击此按钮即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |

手动设置时间： 在这输入正确的时间：小时、分钟、秒、月份、日与年份。

○ **与外部时间服务器同步**
◉ **手动配置时间**

19 **时** 7 **分钟** 1 **秒**
7 **月** 4 **日** 2008 **年**

确定 取消

点击"确认"按钮即会存储刚才所修改的设置内容参数，点击此按钮"取消"即会清除刚才所修改的设置内容参数，此操作必须于确认存储动作之前才会有效。






## 六、广域网络连线设置

本章节讲述基本的广域网络设置，对大多数的用户来说，通过本章节完成基本的设置已经足够连接网络。网络的连接需要一些 ISP 所提供的进一步详细信息。其详细项目设置，请参考以下各节说明：

### 6.1 网络设置



| | |
|---|---|
| 主机名称： | (某些ISP要求输入) |
| 域名： | (某些ISP要求输入) |

**局域网(LAN)接口配置**



| | |
|---|---|
| MAC地址： | 00 - 17 - 16 - 01 - 35 - cf<br>( 默认值: 00-17-16-01-35-cf) |
| 局域网网关： | 10 . 10 . 10 . 1 |
| 子网掩码： | 255 . 255 . 255 . 0 |

**多子网设置**

新增/编辑

| No. | 子网 |
|---|---|
| 掩码 1 | 10.10.10.1 / 255.255.255.0 |

**广域网线路配置**

选择广域网个数：4 (默认值: 4)

| 接口位置 | 连接类型 | 配置 |
|---|---|---|
| 广域网1 | 自动取得 IP 地址 (缆线调制解调器使用者) | 编辑 |
| 广域网2 | 指定 IP 地址 (固接式或ADSL专线使用者) | 编辑 |
| 广域网3 | 自动取得 IP 地址 (缆线调制解调器使用者) | 编辑 |
| 广域网4 | 自动取得 IP 地址 (缆线调制解调器使用者) | 编辑 |

**DMZ 配置**

| 接口位置 | IP地址 | 配置 |
|---|---|---|
| DMZ | 0.0.0.0 | 编辑 |

确定 取消





### 6.1.1 主机名称及域名

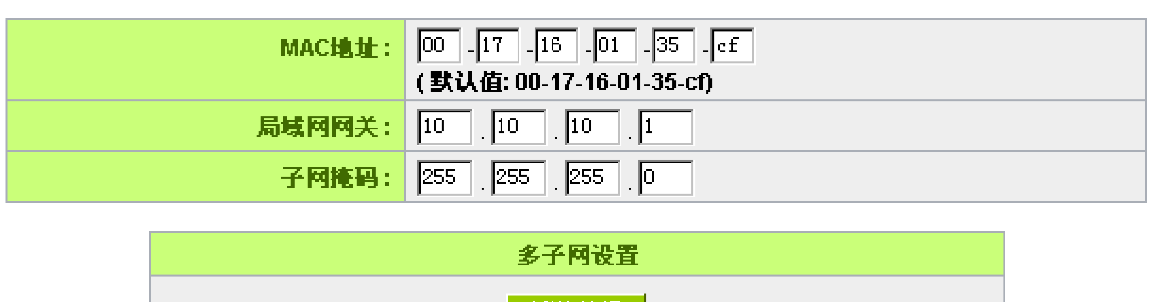
| 主机名称 | SMB | (某些ISP要求输入) |
| --- | --- | --- |
| 网域名称 | smb.com | (某些ISP要求输入) |

可输入 VPN 防火墙的名称（主机名称）以及网域名称，此设置在大多数环境中不需要做任何设置即可使用，除非特殊 ISP 需求！

### 6.1.2 局域网（LAN）接口设置

此为设置 VPN 防火墙的 LAN 端内部网络的 IP 地址，系统默认为 192.168.1.1，子网掩码为 255.255.255.0，您可以依照实际网络架构做变动。

**局域网(LAN)接口配置**





| 多子网设置 | |
| --- | --- |
| 新增/编辑 | |
| No. | 子网 |
| 掩码 1 | 10.10.10.1 / 255.255.255.0 |

Multiple-Subnet 多子网设置：

点击"新增/编辑"按钮弹出多个子网的设置窗口。

局域网IP地址：
子网掩码：
增加到对应列表
删除选中的项目
确定 取消 关闭

此功能是将不同于 VPN 防火墙局域网段的其它网段 IP 加入到 VPN 防火墙认可的局域网段中，这样局域网中的 PC 所在的网段，即使不同于 VPN 防火墙的局域网段，也可以直接上网。举例来说，原来内部环境已经有多组不同的 IP 网段，例如 192.168.3.0， 192.168.20.0， 192.168.150.0 等等，将这些网段加入到子网中，则这些网段的内部计算机不需做任何修改就可以上网，这里可以依照您的实际网络架构运作。

### 6.1.3 广域网络 WAN 及非军事区设置

广域网网络连接型态设置：

**广域网线路配置**

| 接口位置 | 连接类型 | 配置 |
|---|---|---|
| 广域网1 | 自动取得 IP 地址 (缆线调制解调器使用者) | 编辑 |
| 广域网2 | 指定 IP 地址 (固接式或ADSL专线使用者) | 编辑 |
| 广域网3 | 自动取得 IP 地址 (缆线调制解调器使用者) | 编辑 |
| 广域网4 | 自动取得 IP 地址 (缆线调制解调器使用者) | 编辑 |

接口位置：广域网连线所在 WAN 接口位置。






线路连接类型状态：此项显示该广域网口目前设置的联机状态。VPN 防火墙提供五种联机状态设置：自动取得 IP 地址；固定 IP 地址；PPPoE 拨号联机；PPTP 拨号联机以及透明桥接模式。

设置：点击"编辑"按钮可以进入广域网联机状态的设置窗口。各类型的联机状态设置请参考以下的说明，并选择配合 ISP 所给您的联机状态来做设置。

自动取得 IP 地址（动态获得 IP 地址/DHCP 用户）：

此为 VPN 防火墙系统默认的联机方式，此联机方式为 DHCP 客户端自动取得 IP 模式，多为应用于如线缆调制解调器或是 DHCP 客户端联机状态等连接，若您的联机为其它不同的方式，请选取相关的设置并参考以下的介绍做设置。

在自动取得 IP 模式，您可以使用自定 DNS 的 IP 地址，勾选此选项并填入您要使用的 DNS 服务器 IP 地址。

接口位置: WAN1
广域网连接类型: 动态获得 IP 地址(DHCP用户)
☑ 使用以下的DNS服务器IP地址
DNS 服务器(首选): 0 . 0 . 0 . 0
DNS 服务器(备用): 0 . 0 . 0 . 0
☑ 激活掉线排程
广域网掉线时间: 从 : 到 : (时间格式:24小时制)
掉线排程: 分钟前开始转移新的会话
指定备援接口: 关闭
共享式广域网环境: ○ 是 ⦿ 否 (防止收到来自其他广域网的广播封包)
MTU: ⦿ 自动 ○ 手动 1500 bytes
返回 确定 取消

| | |
|---|---|
| 使用以下的 DNS 服务器 IP 地址： | 选择使用自定的 DNS 服务器 IP 地址。 |
| DNS 服务器： | 输入您的 ISP 所提供的动态域名解析服务器 IP 地址，最少填入一组，最多可填二组。 |

| | |
|---|---|
| 广域网掉线排程： | 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 VPN 防火墙有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。 |
| 广域网掉线时间： | 输入此广域网中断连接服务的规则时间。 |
| 掉线排程： | 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。 |
| 指定备援接口： | 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。 |
| 共享式广域网环境： | 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。 |
| MTU: | MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。 |

点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

固定 IP 地址联机（指定 IP 地址）:

若您的 ISP 有核发固定的 IP 地址给您(如 1 个 IP 或是 8 个 IP 等)，请您选择此种方式联机，将 ISP 所核发的 IP 信息分别参照以下介绍填入相关设置参数中。






接口位置: WAN1

广域网连接类型: 指定IP 位址(固定IP或ADSL专线用户)

广域网IP地址: 0 . 0 . 0 . 0

子网掩码: 0 . 0 . 0 . 0

默认网关: 0 . 0 . 0 . 0

DNS 服务器(首选): 0 . 0 . 0 . 0

DNS 服务器(备用): 0 . 0 . 0 . 0

☑ 激活掉线排程

广域网掉线时间: 从 : 到 : (时间格式:24小时制)

掉线排程: 分钟前开始转移新的会话

指定备援接口: 关闭

共享式广域网环境: ○ 是 ⦿ 否 (防止收到来自其他广域网的广播封包)

MTU: ⦿ 自动 ○ 手动 1500 bytes

返回 确定 取消

| | |
|---|---|
| 广域网 IP 地址： | 输入您的 ISP 所核发的可使用固定 IP 地址的其中一个。 |
| 子网掩码： | 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码，如：<br>发放 8 个固定 IP 地址：255.255.255.248<br>发放 16 个固定 IP 地址：255.255.255.240 |
| 默认网关： | 输入您的 ISP 所核发的可使用固定 IP 地址的默认网关 若您是使用 ADSL 的话，一般说来都是 ADSL 数据机（ATU-R）的 IP 地址。 |
| DNS 服务器： | 输入您的 ISP 所规定的名称解析服务器 IP 地址，最少填入一组，最多可填二组。 |
| 广域网掉线排程： | 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 VPN 防火墙有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。 |
| 广域网掉线时间： | 输入此广域网中断连接服务的规则时间。 |





| | |
|---|---|
| 掉线排程： | 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。 |
| 指定备援接口： | 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。 |
| 共享式广域网环境： | 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。 |
| MTU: | MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。 |

点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

PPPoE 拔号联机：

此项为 ADSL 虚拟拨号使用(适用于 ADSL PPPoE)，填入 ISP 给予的使用者联机名称与密码并以 VPN 防火墙内建的 PPP Over Ethernet 软件联机，若是您的 PC 之前已经有安装由 ISP 所给予的 PPPoE 拨号软件的话，请将其移除，不需要再使用此个别连接网络。






接口位置： WAN1

广域网连接类型： PPPoE 设定(ADSL拨接用户)
用户名：
密码：
○ 闲置 5 分钟自动断线.
◉ 保持连接，如断线 30 秒后自动重新连接

☑ 激活掉线排程
广域网掉线时间： 从 : 到 : (时间格式:24小时制)
掉线排程： 分钟前开始转移新的会话
指定备援接口： 关闭
共享式广域网环境： ○ 是 ◉ 否 (防止收到来自其他广域网的广播封包)
MTU： ◉ 自动 ○ 手动 1500 bytes

返回 确定 取消

| | |
|---|---|
| 用户名： | 输入您的 ISP 所核发的使用者名称。 |
| 密码： | 输入您的 ISP 所核发的使用密码。 |
| 闲置( )分钟自动断线： | 此功能能够让您的 PPPoE 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，VPN 防火墙 会自动向默认的 ISP 自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。您可以自行输入所需要的无数据包传送自动离线等待时间，默认为 5 分钟。 |
| 保持连接： | 此功能能够让您的 PPPoE 拨接连线能够断线自动重拨，您可以自行设置重新拨接的时间，默认值为 30 秒。 |
| 广域网掉线排程： | 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 VPN 防火墙有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。 |
| 广域网掉线时间： | 输入此广域网中断连接服务的规则时间。 |

| | |
|---|---|
| 掉线排程： | 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。 |
| 指定备援接口： | 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。 |
| 共享式广域网环境： | 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。 |
| MTU: | MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。 |

点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

PPTP 拨号联机：

此项为 PPTP (Point to Point Tunneling Protocol) 计时制使用，填入 ISP 给予的使用者联机名称与密码并以 VPN 防火墙内建的 PPTP 软件联机。






接口位置: WAN1

广域网连接类型: PPTP 设定(ADSL拨接PPTP用户)
广域网IP地址: 0 . 0 . 0 . 0
子网掩码: 0 . 0 . 0 . 0
默认网关: 0 . 0 . 0 . 0
用户名:
密码:
闲置 5 分钟自动断线.
保持连接，如断线 30 秒后自动重新连接

激活掉线排程
广域网掉线时间: 从 : 到 : (时间格式:24小时制)
掉线排程: 分钟前开始转移新的会话
指定备援接口: 关闭
共享式广域网环境: 是 否 (防止收到来自其他广域网的广播封包)
MTU: 自动 手动 1500 bytes

返回 确定 取消

| | |
|---|---|
| 广域网 IP 地址： | 输入您的 ISP 所核发的可使用固定 IP 地址的其中一个。 |
| 子网掩码： | 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码。 |
| 默认网关： | 输入您的 ISP 所核发的可使用固定 IP 地址的默认网关，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。 |
| 用户名： | 输入您的 ISP 所核发的使用者名称。 |
| 密码： | 输入您的 ISP 所核发的使用密码。 |
| 闲置( )分钟自动断线： | 此功能能够让您的 PPTP 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，VPN 防火墙 会自动向默认的 ISP 自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。无数据包传送的自动离线时间默认为 5 分钟，您可以自行输入所需要的自动离线等待时间。 |
| 保持连接： | 此功能能够让您的 PPTP 拨接连线能够断线自动重拨，而且可以自行设置重新拨接的时间，默认值为 30 秒。 |





| | |
|---|---|
| 广域网掉线排程： | 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 VPN 防火墙有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。 |
| 广域网掉线时间： | 输入此广域网中断连接服务的规则时间。 |
| 掉线排程： | 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。 |
| 指定备援接口： | 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。 |
| 共享式广域网环境： | 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。 |
| MTU: | MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。 |

点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

透通桥接模式（Transparent Bridge）：

当您内网的计算机 IP 已经都是公网 IP 而不希望将内网都改成私网 IP(例如 192.168.1.X)时，此功能可以让您不需更动原有架构，立即整合到既有网络中。选择广域网联机方式为透明桥接模式，这样您可以保留内网计算机的 IP 设置为原本的公网 IP 仍然可以正常上网。

当您设置两个广域网时，广域网的联机模式选择此种透明桥接模式，还是可以做到负载均衡。

接口位置: WAN1

广域网 连接类型: Transparent Bridge (透通桥接模式)
广域网 IP地址: 0 . 0 . 0 . 0
子网掩码: 0 . 0 . 0 . 0
默认网关: 0 . 0 . 0 . 0
DNS 服务器(首选): 0 . 0 . 0 . 0
DNS 服务器(备用): 0 . 0 . 0 . 0
公网IP地址范围 1: 0 . 0 . 0 . 0 到 0
公网IP地址范围 2: 0 . 0 . 0 . 0 到 0

☑ 激活掉线排程
广域网掉线时间: 从 : 到 : (时间格式:24小时制)
掉线排程: 分钟前开始转移新的会话
指定备援接口: 关闭
共享式广域网环境: ○ 是 ⦿ 否 (防止收到来自其他广域网的广播封包)
MTU: ⦿ 自动 ○ 手动 1500 bytes

返回 确定 取消

广域网 IP 地址： 输入您的 ISP 所核发的可使用固定 IP 地址的其中一个。

子网掩码： 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码，如：255.255.255.240

默认网关： 输入您的 ISP 所核发的可使用固定 IP 地址的默认网关，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。

DNS 服务器： 输入您的 ISP 所规定的名称解析服务器 IP 地址，最少填入一组，最多可填二组。

公网 IP 地址范围： 输入您的 ISP 所核发的可使用固定 IP 范围。若是您的 ISP 分给您两个不连续的 IP 地址范围，您可以分别填入。





| | |
|---|---|
| 广域网掉线排程： | 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 VPN 防火墙有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。 |
| 广域网掉线时间： | 输入此广域网中断连接服务的规则时间。 |
| 掉线排程： | 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。 |
| 指定备援接口： | 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。 |
| 共享式广域网环境： | 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。 |
| MTU: | MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。 |

点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

非军事区(DMZ)：

对于某些网络环境应用来说，可能会需要用到独立的 DMZ 非军事管制区接口来置放对外服务服务器，如 WWW 网页服务器与 Mail 电子邮件服务器等等。VPN 防火墙提供您独立的 DMZ 接口来设置连接有合法 IP 地址的服务器。此 DMZ 接口是从网络或局域网存取对外服务器内容的沟通桥梁。

### DMZ 配置

| 接口位置 | IP地址 | 配置 |
|---|---|---|
| DMZ | 0.0.0.0 | 编辑 |

确定　取消

IP 地址：此项显示您给予 DMZ 端口的 IP 地址或范围。






设置：点击"编辑"按钮可以进入 DMZ 的设置窗口。请参考以下的设置说明。

此 DMZ 的设置可分为 Subnet 及 Range 两种：

Subnet（子网）：

DMZ 与广域网络 WAN 要在不同的子网络 Subnet 中。

就是若 ISP 端分配给您 16 个合法 IP 如：220.243.230.1-16/子网掩码：255.255.255.240 时，您必须将此 16 个 IP 再切两组变成 220.243.230.1-8 /子网掩码：255.255.255.248 及另一组 220.243.230.9-16/子网掩码：255.255.255.248，然后 VPN 防火墙及网关是在同一组，再将另一组设置在 DMZ 中。

接口位置: DMZ

⦿ 子网 ○ Range (DMZ与广域网IP地址相同子网掩码)

DMZ IP地址：0 . 0 . 0 . 0
子网掩码：0 . 0 . 0 . 0

Range：

DMZ 与广域网络 WAN 位在相同的子网络 Subnet。

接口位置: DMZ

○ 子网 ⦿ Range (DMZ与广域网IP地址相同子网掩码)

接口位置：广域网2
IP地址范围：220 . 130 . 188 . 0 到 0

IP 地址范围： 输入在 DMZ 端口的 IP 范围。

点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。






## 6.2 多 WAN 设置

当用户的连线是采用多 WAN 的线路设计，管理人员可以进入网络连线设置流量管理以及协议绑定栏目对 VPN 防火墙的负载均衡模式等进行设置，使 VPN 防火墙达到最优数据转发是网络带宽效能达到最高。

### 6.2.1 负载均衡模式

**模式**

| | | |
|---|---|---|
| 智能型负载均衡模式： | ◉ 依会话数均衡 | ○ 依IP地址均衡 |
| 指定路由模式： | ○ 依会话数均衡 | ○ 依IP地址均衡 |
| 策略路由模式： | ○ 依会话数均衡 | ○ 依IP地址均衡 |
| | 广域网組合设定<br>网通策略： 关闭 更新策略<br>自订策略1： 关闭<br>自订策略2： 关闭 | |

智能型负载均衡模式：

当您选用智能负载均衡模式，VPN 防火墙将以会话数或是 IP 地址联机数为基础，并依据您广域网线路的带宽来自动分配联机，达到对外联机的负载均衡。线路的带宽是依据您所填入的带宽设置(请参考下一小节设置说明)，例如当两条广域网都为上行 512Kbit/sec 时，其自动负载比例为 1:1，当一条线路的上行带宽为 1024kbit/sec 另一条为 512kbit/sec 时，则此自动负载比例为 2:1，所以为了确保您的 VPN 防火墙达到实际线路负载能够均衡，请填入实际上行下载带宽 (请参考下一段 QoS 节带宽管理设置说明)。

依会话数均衡：当您选用会话数均衡模式，VPN 防火墙将以会话数为基础，并依据您广域网线路的带宽来自动分配联机，达到联机的负载均衡。

依 IP 地址均衡：当您选用 IP 负载均衡模式，VPN 防火墙将以联机的 IP 数为基础，并依据您广域网线路的带宽来自动分配联机，达到联机的负载均衡。

提示！

不论是联机数均衡或是 IP 负载均衡方式，搭配"通讯协议绑定"可以有更弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务端口作访问，或特定的目的地 IP 经由您指定的广域网来访问外网。

譬如您希望指定 IP 192.168.1.100 访问外网的时候走广域网 1，或内网所有 IP 去访问服务端口

80 时都是经过广域网 2，或是内网所有 IP 去目的地 IP 211.1.1.1 访问时要从广域网 1 去访问等等，都可以经由设置此"通讯协议绑定"功能来达到您的需求。请注意，当使用智能负载均衡方式搭配"通讯协议绑定"功能时，除了您指定的访问会按照您的规则出去访问外网，其它未被指定的 IP 或服务端口的访问还是按照 VPN 防火墙的机制做智能负载均衡。

关于如何设置"通讯协议绑定"功能，以及智能负载均衡方式搭配"通讯协议绑定"的范例，请参考（6.2.3 节的通讯协议绑定设置说明）。

指定路由：

这个模式让您对特定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 经由您指定的广域网对外网做访问。且一经指定后，该广域网也只能让这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 使用。其它不在这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 都会从其它的广域网出去访问。对于没有被指定的广域网，您可以选择他们的负载均衡模式是以联机数作为负载均衡的基础，还是以 IP 联机数作为负载均衡的基础。

未绑定端口均衡模式：若是有部分广网端口并没有被指定，例如广域网 3 与广域网 4 并没有指定特定的 IP、服务端口、或目的 IP 来使用，这些广域网端口(广域网 3 与 4)仍然会依据 VPN 防火墙的负载均衡机制来分配联机。均衡机制如下：

依会话数均衡：当您选用会话数均衡模式，VPN 防火墙将以会话数为基础，并依据您广域网线路的带宽来自动分配联机，达到联机的负载均衡。

依 IP 地址均衡：当您选用 IP 负载均衡模式，VPN 防火墙将以联机的 IP 数为基础，并依据您广域网线路的带宽来自动分配联机，达到联机的负载均衡。

提示！

此指定路由必须配合"通讯协议绑定"功能才能发挥作用。例如指定让内网去访问服务端口 80 时都要从广域网 1 去访问，或内网去目的地 IP 211.1.1.1 访问时要从广域网 1 去访问等等，必须要在"通讯协议绑定"功能中做设置。要注意，当使用指定路由(Exculsive Mode)模式，以上述的例子来看，除了您指定的访问必须按照您的规则出去访问外网都走广域网 1 以外，其它未被指定的 IP 或服务端口则经由 VPN 防火墙负载均衡的机制使用其它的广域网出去。

关于如何设置"通讯协议绑定"功能，以及指定路由模式搭配"通讯协议绑定"的范例，请参考（6.2.3 节的通讯协议绑定设置说明）。

策略路由：

当您选用策略路由模式，VPN 防火墙会依照内建的策略(电信网通分流，用在中国的环境)自动分配联机。





您只需选择网通线路接入的广域网口(或广域网组合)，VPN 防火墙会自动将该走网通线路去外网访问的流量都从网通的广域网出去，对该走电信线路去外网访问的流量也都会往电信的广域网出去，达到"电信走电信，网通走网通"的分流策略。

广域网组合设置：

当您所接的网通线路不只一条，则需要做广域网的组合，以便将两个以上的广域网口合在一起做相同的策略分流。点击"广域网组合设置"会弹出以下的对话窗口。

名称：

接口位置： 广域网1 广域网2 广域网3 广域网4

增加到对应列表

删除选中的项目

确定 取消 关闭

| | |
|---|---|
| 名称： | 在此自定的广域网组合名称，如"教育"等，用来辨识广域网群组。 |
| 接口位置： | 在此勾选要设在此组合的广域网口。 |
| 增加到对应列表： | 增加到广域网组合列表。 |
| 删除选中的项目： | 删除所选择的广域网组合内容。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |
| 关闭： | 关闭并离开此功能设置窗口。 |

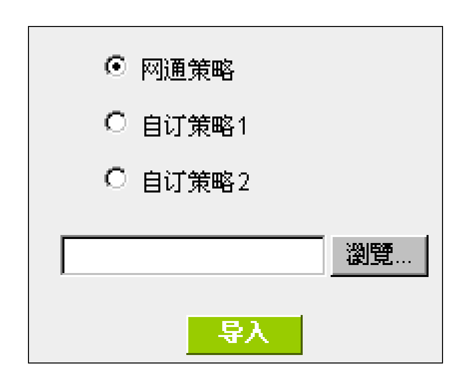
设置完成后，您就可以在网通策略的选择中选取您的网通接口的广域网组合。

自定策略：

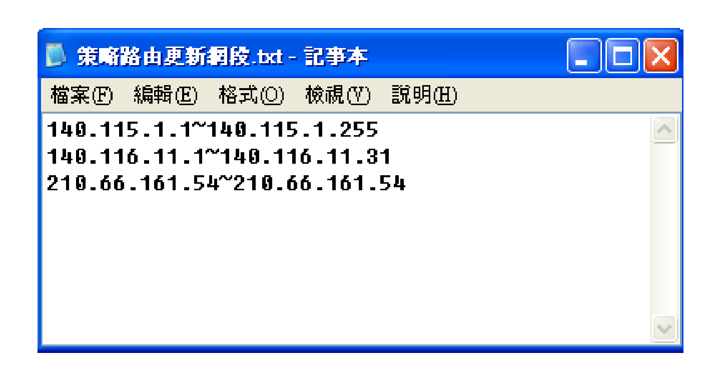





此外，您也可以自己建立分流策略。在"自定策略"中选择要指定的广域网口或广域网组合(例如广域网 1)，然后点击"更新策略"的按键，会出现汇入策略文件的对话窗口。策略文件是一个可编辑的文本文件，应含有您指定的目的 IP 地址。将文件汇入路径选择好之后，点击"汇入"，并在设置窗口的最下方点击"确定"，VPN 防火墙就会将要往指定目的 IP 的流量从您指定的广域网(例如广域网 1)或广域网组合出去。




策略文件的建立可以用纯文本编辑软件来撰写，例如使用 Windows 系统自带的文本编辑程序"记事本"来建立。将您要指定的目的 IP 地址按照下图的格式写入，例如您要指定的目的 IP 地址范围是从 140.115.1.1 到 140.115.1.255，则在"记事本"中输入 140.115.1.1～140.115.1.255。下一个目的 IP 地址范围则要换行输入。请注意！若是只有一个目的 IP 地址，也需要以同样的格式来书写。例如指定的目的 IP 地址是 210.66.161.54，则必须写成 210.66.161.54～210.66.161.54 格式。存储文件后(扩展名应该是.txt)即可汇入自定策略的更新网段。




提示！

网通策略与自定策略可以同时存在，但当某一个目的 IP 同时在网通策略以及自定策略中，则会以网通策略优先执行。也就是说要往该目的 IP 的流量会从网通策略的广域网(或广域网组合)出去外网。

### 6.2.2 线路侦测机制

若勾选此项设置，则会显示出重新发起测试次数，响应延长时间等信息。当使用两条广域网做对外联结线路时一定将此 NSD 启用，以避免因为广域端口流量过大时造成 VPN 防火墙的误判将此线路判断为断线。

## 线路侦测机制

接口位置： 广域网3

| ☑ | 激活 | | |
|---|---|---|---|
| | 重新发起测试 | 5 次 | |
| | 响应延迟时间 | 30 秒 | |
| | 当线路连接失败时 | 记录到日志并移除该条线路 | |
| | ☑ | 当上传 或 下载流量超过 2 % 不进行线路侦测. | |
| | ☑ | 默认网关 | |
| | ☐ | ISP服务器： | |
| | ☐ | 远程服务器： | |
| | ☐ | DNS服务器： | |

接口位置： 选择您要设置线路侦测的广域网口。

重新发起测试次数： 对外联机侦测重试次数，默认值为五次。如果联机侦测重试次数超过设置次数，网络没有回应的话，则判断为对外线路中断！

响应延迟时间： 对外联机侦测逾时时间(秒)，默认值为 30 秒。于此设置秒数之后重新测试对外联机。





当线路连接失败时： 线路连接失败时的处理方式，有两种：

（1）仅记录到日志：当侦测到与 ISP 连结失败时，系统就会在系统日志中将这项错误信息纪录下来，但保持此线路不会移除，所以会导致有些原来使用此条线路上的用户无法正常使用。

此选项适用在当某条广域网联机失败时，从这个广域网去访问的目的地地址是无法从另一条线路去访问的时候，就可以用此选项。例如若是要访问 10.0.0.1 到 10.254.254.254 时一定要走广域网 1 去访问，而且广域网 2 是无法访问到此网段，那就可以使用此选项。因为若广域网 1 掉线后走广域网 2 也无法去访问到 10.0.0.1 到 10.254.254.254，就不需要在广域网 1 断线时将此线路移除。

（2）纪录到日志并移除该条线路：当侦测到与 ISP 连结失败时，系统不会在系统日志中将这项错误信息纪录下来，原本使用此 WAN 端的数据包传递会自动转换到另一条广域端口.等到原本断线的广域端口恢复后会自行重新连结，则数据包传递会自动转换回来。

此选项适用在当某条广域网联机失败时，从这个广域网去访问的目的地位置是可以从另一条线路去访问的时候，就要用此选项。如此可以让任何一条广域网断线的时候，另一条可以做备援，将流量转移到还在联机的广域网。

有流量时不进行侦测： 当下载 或 / 与 上传流量超过带宽的百分之（ ）时，表示线路仍在联机运作，不必再一直送出 NSD 侦测要求数据包

侦测以下可回应的服务器：

默认网关： 近端的默认通讯网关位置，如 ADSL VPN 防火墙的 IP 地址，此为路由自动填入，所以只须打勾选择是否启用。

> 注意！
>
> 有部分的 ADSL 线路的网关是不会响应侦测数据包，或是当您是使用光纤盒，或是运营商发给您的是固定的公网 IP，且网关就是在您网吧这端而不是在运营商那端时，此选项不要启动。

ISP 服务器： ISP 端的侦测位置，如 ISP 的 DNS 服务器 IP 地址等。在设置此 IP 地址时请确认此 IP 地址是可以且稳定快速的得到响应（建议填入 ISP 端 DNS IP)。

远程服务器： 远程的网络节点侦测位置，此 Remote Host IP 地址最好也是可以且稳定快速的得到响应(建议填入 ISP 端 DNS IP)。

DNS 服务器： 网域名称端 DNS 的侦测位置(此字段只许填入网址如"www.hinet.net"，请勿填 IP 地址)。另外，两条 WAN 的此字段不可以填入相同的网址。

确定： 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。

取消： 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。





注意！

在"指定路由"的负载均衡模式下，第一个广域网口会保留给没有指定到其它广域网口(WAN2～WAN8)的 IP 或应用服务端口(服务端口)经由此广域网(WAN1)进出。因此建议您在此模式下将您的其中一条线路接在第一个广域网口。当您其它的广域网口(WAN2～WAN8)断线时，而您在线路侦测机制下选择移除有问题线路，流量就会转移到第一个广域网口(WAN1)。此外，若是第一个广域网口(WAN1)断线，则流量会依次转移到其它广域网口，例如转移到 WAN2，WAN2 也断线则转移到 WAN3 等等。

6.2.3 WAN 口协议绑定设置

带宽设置

VPN 防火墙会依照您实际输入的上传带宽数据作为两条广域端口自动负载平衡的比例依据。例如当两条广域网都为上传 512Kbit/sec 时，其自动负载比例为 1：1。当一条线路的上传带宽为 1024kbit/sec 另一条为 512kbit/sec 时，则此自动负载比例为 2：1。所以为了确保您的 VPN 防火墙达到实际线路负载能够均衡，请填入实际上下载带宽。此段也关系到 QoS 的设置，所以是在 QoS 的页面做设置，请参考相关 QoS 设置章节。

**ISP实际可用带宽**

| 接口位置 | 上传带宽 (Kbit/sec) | 下载带宽 (Kbit/sec) |
|---|---|---|
| 广域网1 | 10000 | 10000 |
| 广域网2 | 10000 | 10000 |
| 广域网3 | 10000 | 10000 |
| 广域网4 | 10000 | 10000 |

协议绑定

使用者可将特定的 IP 或特定的应用服务端口(服务端口)经由您限定的 WAN 出去。其它没有做绑定的 IP 或服务器还是会进行广域网的负载平衡。

注意！

在"指定路由"的负载均衡模式下，第一个广域网口(WAN1)是不能被指定的，保留给没有指定到其它广域网口(WAN2～WAN8)的 IP 或应用服务端口(服务端口)经由此广域网(WAN1)进出。也就是说第一个广域网口(WAN1)不能设置通讯协议绑定的规则，以避免所有的广域网口都被指定有特定的内网 IP、应用服务端口、目的地 IP，导致其它的 IP 或应用服务端口没有广域网口可以使用。





## 协议绑定

服务端口：所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

来源IP地址 10 . 10 . 10 . 0 到 0

目的IP地址：0 . 0 . 0 . 0 到

0 . 0 . 0 . 0

接口位置：广域网1

激活：

上移　增加到对应列表　下移

FTP [TCP/21~21]->10.10.10.0~0(0.0.0.0~0.0.0.0)广域网1

删除选中的项目

显示开启表　确定　取消

服务端口： 在此选择欲开启的绑定服务端口，从下拉式选单中可以选择默认列表(如 All -TCP&UDP 0～65535， WWW 为 80～80， FTP 为 21～21 等等)，默认的服务为 All 0～65535。

点击"服务端新增或删除表"按钮可以进入服务端口设置窗口，进行新增或删除选单中默认的服务端口。

来源 IP 地址： 您可以指定特定的内部虚拟 IP 地址的数据包经由特定的广域端口出去。

在此填上内部虚拟 IP 地址范围，例如 192.168.1.100 到 150.则 IP 地址 100 到 150 为绑定范围。如果使用者只需要设置特定的服务端口而不需指定特定的 IP 地址， 则在 IP 的字段皆填入 0。您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设置，请参考（"7.6 IP 群组管理"的说明）。

| | |
|---|---|
| 目的 IP 地址： | 在此填上外部固定 IP 地址，例如若有一目标地址 210.11.1.1，要连接此地址的使用者限定只能从广域端口 1 到达此目标地址，则在此填上外部固定 IP 地址 210.11.1.1 到 210.11.1.1。如果使用者要设置一个范围的目的地位置，则填入方式可以为 210.11.1.1 到 210.11.255.254，则表示整组 210.11.x.x 的 Class C 网段都限制走某一条广域网，若只需要设置特定的应用而不需指定特定的 IP 地址，则在 IP 的字段皆填入 0.0.0.0。 |
| 接口位置： | 选择您所要绑定此条规则在哪一个 WAN 端口。 |
| 激活： | 启用此规则。 |
| 增加到对应列表： | 增加此条规则到列表。 |
| 删除选中的项目： | 删除在服务列表里所选择的规则。 |
| 上移 & 下移： | 由于每条规则执行的优先级为由列表的最上面那条往下执行，也就是越后面设置的规则会越后执行，所以您可以自行调整每条规则先后执行顺序。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |

---

注意！

通讯绑定协议所设的规则在 VPN 防火墙执行时也有优先级的，由上到下，在列表上最上方那条会先执行，然后依序往下。

---

显示开启表：

按下"显示开启表"，会出现以下的对话窗口。您可以选择以"优先级"来显示排列的顺序，或是以"接口位置"来显示排列的顺序。点击"刷新"可以重新显示窗口，点击"关闭"将结束这个对话窗口。

◉ 优先级 ○ 接口位置 刷新 关闭

| 优先级 | 接口位置 | 服务端口 | 来源IP地址 | 目的IP地址 | 激活 | 编辑 |
|---|---|---|---|---|---|---|
| 1 | 广域网1 | FTP [TCP/21~21] | 10.10.10.0~10.10.10.0 | 0.0.0.0~0.0.0.0 | 激活 | 编辑 |

新增或删除管理服务端口号

若您欲开启的服务端口项目没有在表列中，您可以点击"服务端口新增或删除表"按钮，新增或删除管理服务端口号列表，如以下所述：






服务名称：

通讯协议： TCP

端口范围： 到

增加到对应列表

所有端口 [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
SMTP [TCP/25~25]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]
TELNETSSL [TCP/992~992]
DHCP [UDP/67~67]
L2TP [UDP/1701~1701]

删除选中的项目

确定 取消 关闭

| | |
|---|---|
| 服务端口名称： | 在此自定欲开启的服务端口号名称加入列表中，如 BT 等。 |
| 通讯协议： | 在此选择欲开启的服务端口号的数据包格式为 TCP 或 UDP。 |
| 服务端口的位置范围： | 填入您将新增加的服务端口范围。 |
| 增加到对应列表： | 增加到开启服务项目内容列表，最多可新增 100 组。 |
| 删除选中的项目： | 删除所选择的开启服务项目内容。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |
| 关闭： | 离开并关闭此功能设置窗口。 |

使用"智能型"负载均衡模式时其通讯协议绑定协议设置方式：

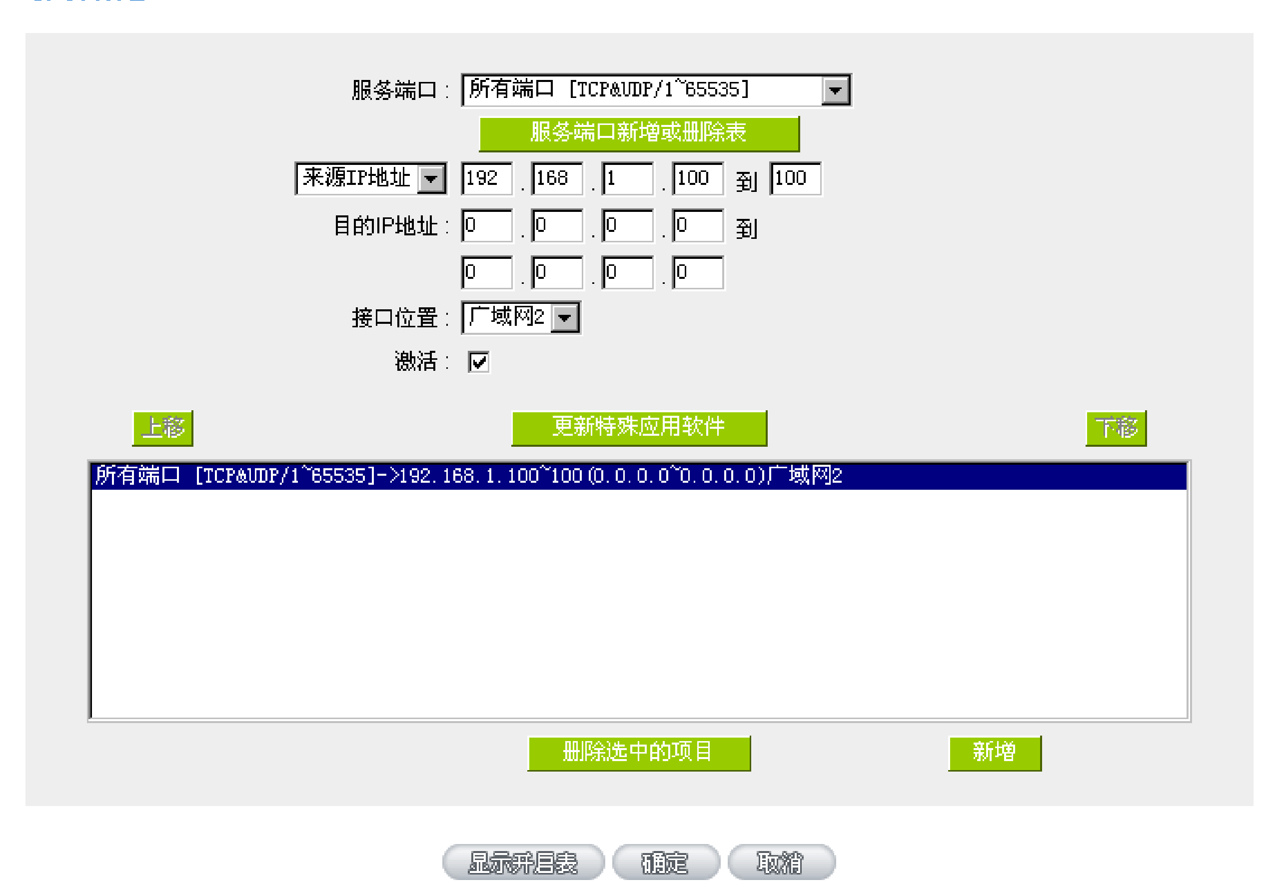
智能负载均衡方式搭配"通讯协议绑定"可以有更弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务端口作访问，或特定的目的地 IP 经由您指定的广域网来访问外网。





范例一：若要指定内网 IP 192.168.1.100 去外网访问都走广域网 2，那通讯协议绑定设置方式?

如以下范例所示，服务端选择"所有端口"，在来源 IP 地址填入 192.168.1.100 到 100，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选激活。最后点击"新增"即可将此规则加入。




范例二:若要指定内网 IP192.168.1.150 到 200 去外网访问 80 端口都走只能走广域网 2 去访问，那通讯协议绑定怎样设置?

如以下范例所示，服务端选择"HTTP[TCP/80~80]"，在来源 IP 地址填入 192.168.1.150 到 200，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选激活。最后点击"新增"即可将此规则加入。

## 协议绑定

| | |
|---|---|
| 服务端口： | HTTP [TCP/80~80] |
| | 服务端口新增或删除表 |
| 来源IP地址 | 192 . 168 . 1 . 150 到 200 |
| 目的IP地址： | 0 . 0 . 0 . 0 到 |
| | 0 . 0 . 0 . 0 |
| 接口位置： | 广域网2 |
| 激活： | ☑ |

上移　更新特殊应用软件　下移

HTTP [TCP/80~80]->192.168.1.150~200(0.0.0.0~0.0.0.0)广域网2

删除选中的项目　新增

显示开启表　确定　取消

<u>范例三：若要指定内网所有 IP 去外网访问 80 端口都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定是怎样设置?</u>

如以下范例所示，要设置两条规则：

第一条规则服务端选择"HTTP[TCP/80~80]"，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选激活。最后点击"新增"即可将此规则加入。VPN 防火墙会将所有用 80 端口去外网访问的流量都走广域网 2，但是不是用 80 端口的流量根据 VPN 防火墙的自动负载平衡演算，还是有可能会走广域网 2，因此还需要再设第二条规则。

第二条规则，服务端选择"所有端口[TCP&UDP/1~65535]"，在来源 IP 地址填入 192.168.1.2 到 254，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 1，然后勾选激活。最后点击"新增"即可将此规则加入。这时 VPN 防火墙会将不是用 80 端口去外网访问的流量都走广域网 1。





## 协议绑定

服务端口：HTTP [TCP/80~80]
服务端口新增或删除表
来源IP地址 192 . 168 . 1 . 0 到 0
目的IP地址：0 . 0 . 0 . 0 到
0 . 0 . 0 . 0
接口位置：广域网2
激活：☑
上移 更新特殊应用软件 下移
HTTP [TCP/80~80]->192.168.1.0~0(0.0.0.0~0.0.0.0)广域网2
所有端口 [TCP&UDP/1~65535]->192.168.1.2~254(0.0.0.0~0.0.0.0)广域网1
删除选中的项目 新增
显示开启表 确定 取消

使用"指定路由"的负载均衡模式时其通讯协议绑定协议设置方式：

指定路由的模式让您对特定的内网 IP、特定要访问的应用服务端口或特定目的地 IP 经由您指定的广域网对外网做访问。且一经指定后，该广域网也只能让这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 使用。其它不在这些指定内的内网 IP、特定要访问的应用服务端口或特定目的地 IP 都会从另一条广域网出去访问。此模式必须配合"通讯协议绑定"功能才能发挥作用。

范例一：若要指定内网所有 IP 去外网访问 80 端口都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定设置方式是怎样设置?

如以下范例所示设置规则，服务端选择"HTTP[TCP/80~80]"，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选激活。最后点击"新增"即可将此规则加入。此时广域网 2 只会有访问外网 80 端口的流量，其余流量都只走广域网 1。





## 协议绑定

服务端口：HTTP [TCP/80~80]

服务端口新增或删除表

来源IP地址 192 . 168 . 1 . 0 到 0

目的IP地址 0 . 0 . 0 . 0 到

0 . 0 . 0 . 0

接口位置：广域网2

激活：☑

上移　更新特殊应用软件　下移

HTTP [TCP/80~80]->192.168.1.0~0(0.0.0.0~0.0.0.0)广域网2

删除选中的项目　新增

显示开启表　确定　取消

<u>范例二：若要指定内网所有 IP 去外网访问 IP 211.1.1.1 到 211.254.254.254 还有 60.1.1.1 到 60.254.254.254 整组 A 类段时都走走广域网 2 去访问，但去其余不是这几个目的地 IP 段时都走广域网 1 时，那通讯协议绑定设置方式如何设置?</u>

如以下范例所示设置两条规则：

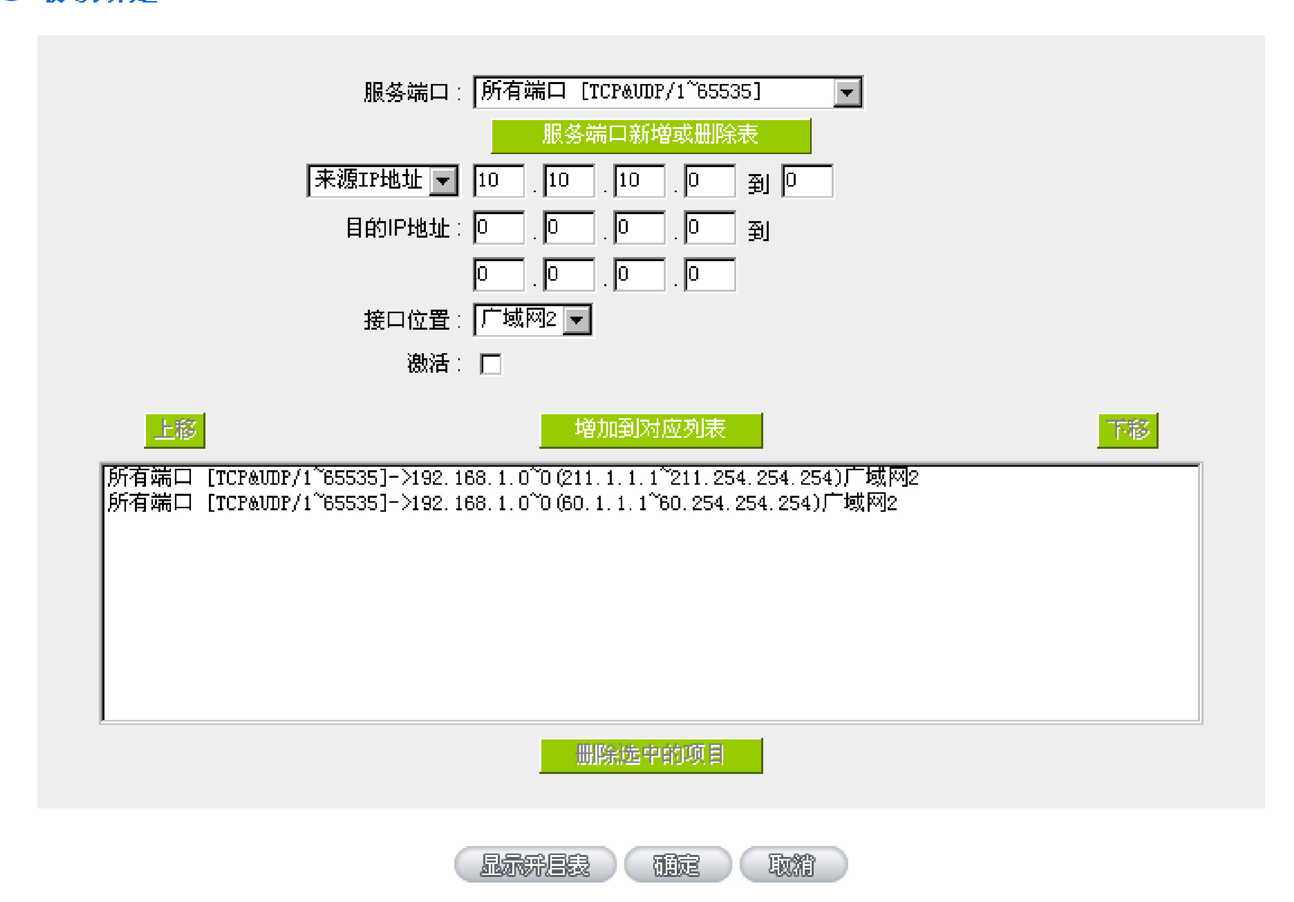
第一条规则中服务端选择"所有端口[TCP&UDP/1~65535]"，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址填入 211.1.1.1 到 211.254.254.254。接口位置选则广域网 2，然后勾选激活。最后点击"新增"即可将此规则加入。

第二条规则中服务端选择"所有端口[TCP&UDP/1~65535]"，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址填入 60.1.1.1 到 60.254.254.254。接口位置选则广域网 2，然后勾选激活。最后点击"新增"即可将此规则加入。此时，除了上述两条规则所涵盖的目的 IP，其余去外网访问的流量都只走广域网 1。





## 协议绑定


服务端口：
所有端口 [TCP&UDP/1~65535]
服务端口新增或删除表
来源IP地址
到
目的IP地址：
到
接口位置：
广域网2
激活：
上移
增加到对应列表
下移
所有端口 [TCP&UDP/1~65535]->192.168.1.0~0(211.1.1.1~211.254.254.254)广域网2
所有端口 [TCP&UDP/1~65535]->192.168.1.0~0(60.1.1.1~60.254.254.254)广域网2
删除选中的项目
显示开启表
确定
取消



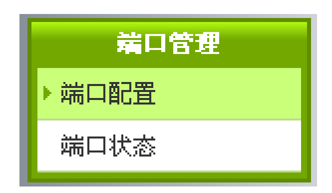


七、内部局域网络设置

通过本章节可以对端口进行设置管理，了解如何设置内部局域网络的 IP 地址。

## 7.1 网络端口管理设置

VPN 防火墙，管理者可以设置网络实体联机于每一个以太网络端口，如连接速率，工作模式，优先级，自动翻转或是 VLAN 等以太网络端口的功能。




### 端口配置

选择广域网个数：4 (默认值: 4)

☐ 激活镜像端口(Port 1)

| 端口号 | 接口位置 | 关闭 | 优先级 | 连接速率 | 半双/全双工模式 | 自动翻转功能 | VLAN |
|---|---|---|---|---|---|---|---|
| 1 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 2 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 3 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 4 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 5 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 6 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 7 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 8 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 9 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 10 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 11 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 12 | LAN | ☐ | Normal | 100M | 全双 | ☑ | VLAN1 |
| 13 | WAN4 | ☐ | Normal | 100M | 全双 | ☑ | |
| 14 | WAN3 | ☐ | Normal | 100M | 全双 | ☑ | |
| 15 | WAN2 | ☐ | Normal | 100M | 全双 | ☑ | |
| 16 | WAN1 | ☐ | Normal | 100M | 全双 | ☑ | |

确定 取消

镜像端口：勾选"激活镜像端口（Port 1）"可以将局域网的第一个端口设置为镜像端口，所有从内网到外






网访问的流量都会复制到镜像端口。因此您可以将监控或是过滤服务器直接接在镜像端口，来达到监控或是过滤网络数据包的目的。一旦您激活这个功能，首页中的"端口设置状态"会显示端口 1 为"镜像端口"。如下图：

### 端口配置状态

| 端口号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 接口位置 | 镜像端口 | 局域网 | | | | | | |
| 状态 | 激活 | 激活 | 激活 | 激活 | 激活 | 激活 | 激活 | 激活 |

| 端口号 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | DMZ |
|---|---|---|---|---|---|---|---|---|
| 接口位置 | 局域网 | | | 广域网4 | 广域网3 | 广域网2 | 广域网1 | DMZ |
| 状态 | 激活 | 激活 | 激活 | 激活 | 激活 | 连接 | 激活 | 激活 |

关闭端口： 此为设置以太网络的 LAN 端口开启或是关闭的功能，若是打勾的话，则此以太网络端口立即被关闭无法连接使用。默认为开启无打勾。

优先级设置： 此为设置此以太网络的 LAN 端口数据包传送优先权设置，若是此端口设置为高的话，则最优先使用传送数据包的权利，默认优先级为一般。

网络端口连接速度： 此为设置此以太网络的端口网络实体连接速率选项，您可以设置为 10Mbps 或是 100Mbps 连接速度。默认为自动侦测。

半双/全双工模式： 此为设置此以太网络的端口网络实体连接速率工作模式选项，您可以设置为半双工模式或是全双工模式运作。默认为自动侦测。

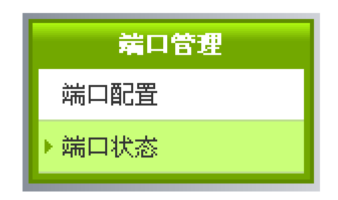
自动翻转功能： 此为设置以太网络的端口网络实体连接速率自动侦测模式，若是勾选的话，自动侦测所有连接端口的信号与调整。

VLAN： 此功能可以让网管人员在自己的局域网内将每一个局域网端口设置 1 个或多个不同网段且无法互通的局域网端口，但都可以通过 VPN 防火墙上网络。在同一个网段内的成员(在同一个 VLAN 局域网络内)可互相沟通并看得到对方，若不在同一个 VLAN 群组内的成员则无法得知其它成员的存在。使用者可为每一个 LAN 端口选定为哪一个 VLAN 局域网络群组。

VLAN All： 当网管人员在内网设置了多个 VALN 端口，且不在同一个 VLAN 群组内无法互访，可是内网又需要架设服饰器让内网所有 VLAN 群组都可以访问此服务器。此时可以将某一局域网端口设置为 VLAN All，将此服务器接入此 VLAN All 的端口，这样就可以让所有不同 VLAN 群组的计算机都可以访问到此服务器。

7.2 网络端口状态实时显示

此项功能可以让网络管理者查看每个实体端口的详细信息。




端口号：2

**摘要信息**

| 网路连接状态 | 10Base-T / 100Base-TX |
| --- | --- |
| 接口位置 | 局域网 |
| 线路连线状态 | 关闭 |
| 端口配置状态 | 端口激活 |
| 优先级设定 | 一般 |
| 连接速率 | 10 Mbps |
| 半双/全双工模式 | 半双工 |
| 自动翻转功能 | 激活 |
| VLAN | VLAN1 |

**流量实时状态**

| 接收数据包统计 | 0 |
| --- | --- |
| 数据包接收Byte数量 | 3052672 |
| 传送数据包统计 | 0 |
| 数据包传送Byte数量 | 3204100 |
| 错误数据包统计 | 0 |

刷新

整体资讯项目：

网路连接状态（10Base-T / 100Base-TX / 1000Base-T）， 接口位置（局域网/广域网络/DMZ），线路连线状态(激活/关闭)，端口设置状态（端口激活/端口关闭），优先级设置（高级/一般），网路连接速率（10Mbps/100Mbps/1000Mbps），半双/全双工模式(半双工/全双工)，自动翻转功能（激活/关闭），VLAN（VLAN Number / VLAN All）。





端口流量实时状态：

即时显示 VPN 防火墙工作状态下的接收和传送数据包计算、数据包接收和传送 Byte 数以及错误数据包统计实际数值。






## 7.3 DHCP 发放 IP 服务器

VPN 防火墙的 DHCP 服务器，默认值是启动，可以提供局域网络内的计算机自动取得 IP 的功能，(如同 NT 服务器中的 DHCP 服务)，好处是每台 PC 不用去记录与设置其 IP 地址，当计算机开机后，就可从 VPN 防火墙自动取得 IP 地址，管理方便。



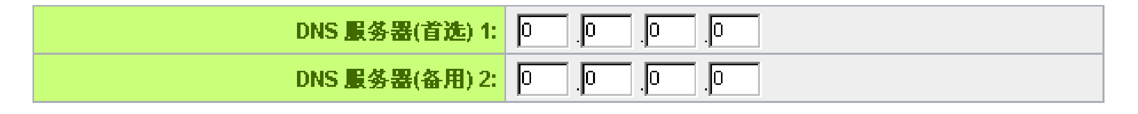

☑ 激活 DHCP服务器

DHCP 用户使用IP范围

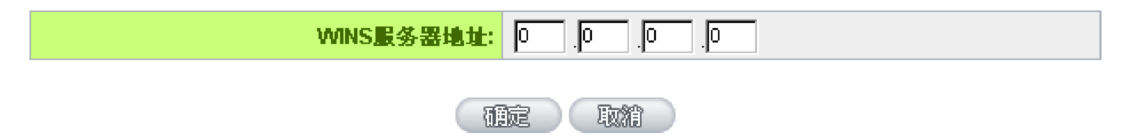



| |
|---|
| 起始IP地址：10 . 10 . 17 . 100 |
| 结束IP地址：10 . 10 . 17 . 149 |

域名解析服务(DNS)




WINS服务器







动态 IP 服务：

| | |
|---|---|
| 租约时间： | 此设置为发给 PC 端 IP 地址的租约时间，默认为 1440 分钟(代表时间为一天)，当租约时间到后，PC 端会重新跟路由再申请一次。您可以依照实际需求来设置。 |
| 起始 IP 地址： | 系统默认为四个网段从 192.168.0.100、192.168.1.100、192.168.2.100、192.168.3.100 的 IP 地址开始发放。您可以依照实际需求来设置。 |
| 结束 IP 地址： | 系统默认为四个网段 192.168.0.149、192.168.1.149、192.168.2.149、192.168.3.149IP 地址为最后发放 IP，也就是说出厂设置值每个网段可供 50 台计算机自动取得 IP 地址，四个网段共 200 台计算机自动取得 IP 地址。您可以依照实际需求来设置。 |

域名解析服务（DNS）地址：

此设置为发给 PC 端 IP 地址的 DNS 网域服务器查询地址，若您有特定使用的 DNS 服务器，可以直接输入此服务器的 IP 地址，则 PC 端从 DHCP 取得 IP 地址时，也会一并取得指定的 DNS 服务器地址。

| | |
|---|---|
| DNS 服务器（首选）1： | 输入 DNS 网域服务器的 IP 位置。 |
| DNS 服务器（备用）2： | 输入 DNS 网域服务器的 IP 位置。 |

WINS 服务器：

若您的网络上有解析 Windows 计算机名称的服务器，您可以直接输入此服务器的 IP 地址。

| | |
|---|---|
| WINS 服务器地址： | 输入 WINS 网域服务器的 IP 位置。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |

## 7.4 DHCP 状态显示

此状态表为显示 DHCP 服务器的目前使用状态与设置纪录等，以便提供管理人员需要时做网络设置参考数据。




### 状态

| | |
|---|---|
| DHCP服务器： | 10.10.10.1 |
| 已使用的动态IP数量： | 0 |
| 已发放的固定IP数量： | 0 |
| 剩余可用的IP数量： | 50 |
| 可发放的IP总量： | 50 |

### DHCP 用户连接列表

| 主机名称 | IP地址 | MAC地址 | 租约到期时间 | 删除 |
|---|---|---|---|---|

刷新

| | |
|---|---|
| DHCP 服务器 IP 地址: | 目前 DHCP 服务器的 IP 地址。 |
| 已使用的动态 IP 数量： | 目前 DHCP 服务器已经发放动态 IP 的数量。 |
| 已发放的固定 IP 数量: | 目前 DHCP 服务器已经发放固定 IP 的数量。 |
| 剩余可用的 IP 地址: | 目前 DHCP 服务器可以还可发放的 IP 数量。 |
| 可发放的 IP 总量: | 目前 DHCP 服务器所设置可发放的 IP 总数量。 |
| 主机名称: | 目前此台计算机的计算机名称。 |
| IP 地址: | 目前此台计算机所取得的 IP 地址。 |
| MAC 地址: | 目前此台计算机的 MAC 网络实体位置。 |
| 租约到期时间: | DHCP 目前核发 IP 地址的租约时间。 |
| 删除: | 删除此笔核发 IP 纪录。 |





## 7.5 IP 及 MAC 地址绑定

在许多的大中型网吧及企业网络中，网管人员可以设置 VPN 防火墙所提供的 IP & MAC 绑定功能，达到用户不能自行添加计算机来使用对外网络或是私自擅改 IP 上网影响他人。另外通过此功能也可以将每台计算机或服务器的 MAC 地址绑定，达到计算机或服务器每次开机或重新要 IP 时，都分配给它相同的一组 IP 地址。




IP与MAC绑定

显示新加入的IP地址

静态IP地址 :

所对应的MAC地址 :

名称 :

激活 :

增加到对应列表

删除选中的项目

封锁绑定列表中IP地址与MAC地址不对应的用户

封锁未绑定或绑定列表中未激活的用户

显示开目表 确定 取消

您可以以两种方式来设置这个功能：






限定可以使用网络的 MAC 地址

此功能主要目的是限制只有在列表里面的 MAC 地址才可以得到 DHCP 分配的 IP 地址上网，未在此列表的计算机都无法取得 IP 上网；或是限制有在列表但是未激活绑定功能的计算器。当使用此功能时，切记要将静态 IP 地址填 0.0.0.0 不可以空白，另外将"封锁未绑定或绑定列表中未激活的用户"选项勾选才可以执行。如下图中范例所示：

**IP与MAC绑定**

显示新加入的IP地址

静态IP地址 : . . .

所对应的MAC地址 : - - - - -

名称 :

激活 : ☐

增加到对应列表

删除选中的项目

☐ 封锁绑定列表中IP地址与MAC地址不对应的用户

☑ 封锁未绑定或绑定列表中未激活的用户

显示开目表 确定 取消

IP 及 MAC 地址绑定

此功能主要目的是让指定的 MAC 地址计算机在每次开机都会要到同一个指定 IP。此外，若将"封锁绑定列表中 IP 地址与 MAC 地址不对应的用户" 功能启用，那么设置为固定 IP 的计算机或通过此功能已发给特定 IP 的计算机擅自更改 IP 为非指定的 IP 地址时，则会无法上网。






## IP与MAC绑定

显示新加入的IP地址

静态IP地址 : _ . _ . _ . _

所对应的MAC地址 : _ - _ - _ - _ - _ - _

名称 :

激活 : ☐

增加到对应列表

删除选中的项目

☑ 封锁绑定列表中IP地址与MAC地址不对应的用户

☑ 封锁未绑定或绑定列表中未激活的用户

显示开启表　确定　取消

| | |
|---|---|
| 静态 IP 地址设置： | 此字段有两种填入方式：<br>1. 若您只要限制 MAC 地址可以跟 DHCP 要 IP 而不一定是指定的那一个 IP，请在此字段填 0.0.0.0，不可为空白。<br>2. 若要求每次此台计算机都要分配到同一个 IP，则将您所要求分配给此台计算机的 IP 地址输入。这样所要绑定服务器或 PC 端每次重启都会要到固定的同一个虚拟 IP。 |
| 所对应的 MAC 地址: | 输入要绑定的服务器或 PC 端固定实体 MAC(网络卡上的地址)。 |
| 名称: | 填入您所绑定此用户的名字或地址做辨识，可输入 12 个字符，中英文皆可以。 |
| 激活: | 启用此组设置。 |
| 增加到对应列表: | 增加或修正此设置到列表中。 |
| 删除选中的项目: | 删除列表中所选择的绑定。 |
| 新增: | 当列表中有绑定规则后，右下角会出现此按钮，可点击增加新的绑定。 |





封锁绑定列表中 IP 地址与 MAC 地址不对应的用户：此选项打勾后，只要是 User 自行更改计算机的 IP 或不是列表设置的 IP 将无法上网。

封锁未绑定或绑定列表中未激活的用户：此选项打勾后，只要不在列表中或是在列表中未激活绑定功能的 MAC 地址都无法上网。

显示出还未做绑定或新加入的 IP 及其 MAC 地址：

此功能的主要目的是为了减少网管人员需一一查询每台计算机的 MAC 地址后才能进行绑定，因为会非常耗时且困难。再者，将 MAC 地址手动填入列表也很容易出错。所以只需要查询此表格，就可以看到所有进出 VPN 防火墙且还未绑定的 MAC 地址，然后直接在此表格做绑定动作即可。另外，若您发现此表格出现已经绑定的某组 MAC 又出现在此表格，则表示此用户试图修改不是您指定的 IP 上网。

新加入的IP 地址列表 - Windows Internet Explorer

http://220.130.188.40/Dhcp_table1.htm

确定 全选 刷新 关闭

| IP地址 | MAC地址 | 名称 | 激活 |
|---|---|---|---|
| 10.10.10.104 | 00:17:16:01:f0:b2 | | ☐ |
| 10.10.10.103 | 00:17:16:01:66:b3 | | ☐ |
| 10.10.10.101 | 00:0e:a0:00:1d:a3 | | ☐ |
| 10.10.10.100 | 00:01:80:37:fb:c3 | | ☐ |
| 10.10.10.107 | 00:1b:24:d1:af:15 | | ☐ |
| 10.10.10.105 | 00:17:16:00:a6:68 | | ☐ |
| 10.10.10.106 | 00:17:16:00:c6:8b | | ☐ |
| 10.10.10.100 | 00:11:2f:5a:ac:9c | | ☐ |
| 10.10.10.102 | 00:17:16:01:94:3e | | ☐ |

完成 網際網路 100%

名称:　　可以填入您所绑定此用户的名字或地址做辨识，可输入 12 个字符。

激活　　勾选您所要绑定的目标。

确定:　　将您所选定好的目标绑定到 IP & MAC 绑定列表。

全选　　选择所有在此列表中的目标做绑定。

刷新：　　更新此列表。

关闭:　　关闭此列表。






## 7.6 IP 群组管理

IP 群组功能可以让您将数个 IP 地址或 IP 地址范围组合成一个群组。当您以 IP 地址来管理使用者的网络存取权限的时候，您可以将具有相同使用权限的使用者设置在同一个 IP 群组里，并在各个管理功能中选择以 IP 群组的方式来做设置，可以减少以单一 IP 来做设置的规则数。例如在"通讯协议绑定"的设置，"带宽管理(QoS)"的设置，以及"访问规则"的设置中，都可以选择以 IP 群组的方式来做设置，如此就不需要再以单一 IP 来设置，减少所需要的规则数。

### IP 群组管理

群組配置

IP群組 : 新增群組 删除群組

群組名称 :

IP地址 : 10 . 10 . 10 . 到

增加到对应列表

删除选中的项目

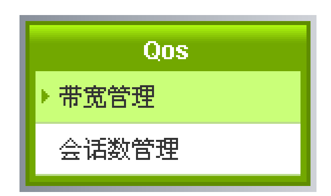
| | |
|---|---|
| IP 群组: | 当您已经有建立好的 IP 群组，您可以在此字段选择要修改的群组名称。 |
| 新增群组： | 点击此按钮可以建立新的 IP 群组。 |
| 删除群组： | 将您所选定的 IP 群组删除。 |
| 群组名称： | 在此字段输入您要建立的 IP 群组名称，或是修改已经建立过的 IP 群组名称。 |
| IP 地址： | 在此字段输入您要建立的 IP 群组的 IP 地址，或是修改已经建立过的 IP 群组的 IP 地址。 |
| 增加到对应列表： | 加入或修正此设置到列表中。 |
| 删除选中的项目： | 删除列表中所选择的群组。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于"确定"存储动作之前才会有效。 |





八、QoS 带宽管理功能

带宽管理 QoS 为 Quality of Service 缩写，其功能主要为限制某些服务及 IP 的带宽使用量，以满足特定应用程序或服务所需要的带宽或优先权，并让其余的使用者共享带宽，才能有比较稳定、可靠的数据传送服务。网络管理人员应该针对网吧、企业等的实际需求，对各种不同网络环境、应用程序或服务来进行带宽管理，才能充分且有效率的达到网络带宽使用。







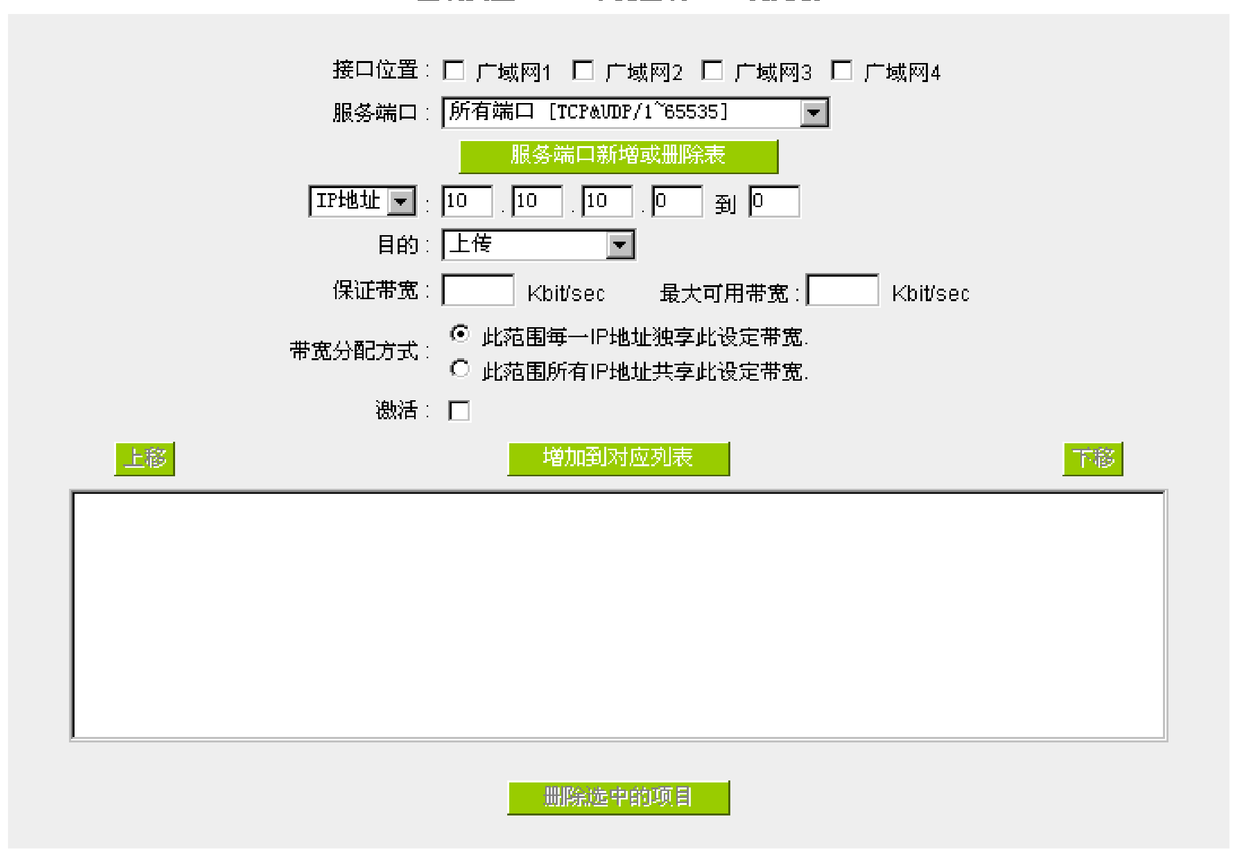
## 8.1 带宽设置(QoS)

### ISP实际可用带宽

| 接口位置 | 上传带宽 (Kbit/sec) | 下载带宽 (Kbit/sec) |
|---|---|---|
| 广域网1 | 10000 | 10000 |
| 广域网2 | 10000 | 10000 |
| 广域网3 | 10000 | 10000 |
| 广域网4 | 10000 | 10000 |

### QoS带宽管理

控制类型： ⦿ 带宽控制 ○ 优先级




☐ 激活动态智能QoS

显示开目表　确定　取消

8.1.1 带宽设置

**ISP实际可用带宽**

| 接口位置 | 上传带宽 (Kbit/sec) | 下载带宽 (Kbit/sec) |
|---|---|---|
| 广域网1 | 10000 | 10000 |
| 广域网2 | 10000 | 10000 |
| 广域网3 | 10000 | 10000 |
| 广域网4 | 10000 | 10000 |

WAN 的带宽数据请填入您所申请的宽带网络实际上传及下载带宽，QoS 的带宽控制会依照您所填入的带宽作为计算依据。例如每个 IP 及服务端口（服务端口）可以保障使用的上传或下载的最小带宽会依照此 WAN1 及 WAN2 的实际带宽相加来换算实际可保障的大小。例如上传带宽若两条都为 512Kbit/Sec，那实际上传带宽就为 WAN1+WAN2=1024Kbit/Sec，所以若有 50 个 IP 在内部网络，若要保证每人最小可使用的上传带宽，则就把 1024Kbit/50=20Kbit，这样每人可以保证的最小带宽就可以填 20kbit/Sec，下载同此换算方式。

注意！

这里的数值单位是 kbit，有些应用软件显示下载/上传速度单位为 KB，两个数值之间的换算方式为 1KB=8kbit。

8.1.2 QoS 设置

QoS 可以选择两种方式并且同时使用，一为流量控制(带宽管理)，另一个为优先权控制，设置人员可以依照自己内网需求做两种模式灵活运用。

带宽控制 (带宽管理) - 依使用量做管理：

网管人员可依照您现有的带宽大小做每一个 IP 或一个范围的 IP 的使用量限制或保障带宽。另外也可以针对服务端口去做带宽控制。若是内部有架设服务器的话，也可控制或保障其对外带宽。

## QoS带宽管理

**控制类型：** ⊙ **带宽控制** ○ **优先级**

接口位置： ☐ 广域网1 ☐ 广域网2 ☐ 广域网3 ☐ 广域网4

服务端口： 所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

IP地址 ： 10 . 10 . 10 . 0 到 0

目的： 上传

保证带宽： Kbit/sec 最大可用带宽： Kbit/sec

带宽分配方式： ⊙ 此范围每一IP地址独享此设定带宽. ○ 此范围所有IP地址共享此设定带宽.

激活： ☐

上移 增加到对应列表 下移

删除选中的项目

接口位置：

勾选此条 QoS 设置要控制在哪条 WAN 执行，可单独或全部勾选。

服务端口：

选择此条 QoS 所要设置的带宽控制为哪个，若您是要针对每个 IP 的所有服务的使用带宽，则将此选择在 All(TCP&UDP)1~65535。若您只要针对譬如 FTP 上传或下载，其余服务不限制，则选择 FTP Port21~21，可参考服务号码默认列表。





| | |
|---|---|
| IP 地址： | 此为选择您所要限制的使用者为哪些?若您只限制单一 IP，则直接将此 IP 填入，如：192.168.1.100 到 100，则此规则就是针对 192.168.1.100 此 IP 做控制。若是要限制一组 IP 范围，则填入如 192.168.1.100 到 150，这样此规则就是针对 192.168.1.100 到 150 做限制。若是此条带宽限制是针对所有人也就是接在 VPN 防火墙内网的所有 User 则可在 IP 的字段皆填入 0，也就是 192.168.1.0 到 0，这样就表示所有 IP 都受此规则限制。另外此 QoS 是可以控制到 Class C 的范围。<br><br>您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设置，请参考（"5.4 IP 群组管理"的说明）。 |
| 目的： | 上传： 指对内网 IP 的上传带宽<br><br>下载： 指对内网 IP 的下载带宽<br><br>虚拟服务器上传(Server in LAN，上传)：若您有架设对外的 Server 网站在 VPN 防火墙内部，则此选项为控制外部访问此 Server 的带宽控制。<br><br>虚拟服务器下载(Server in LAN，下载)：若您有架设网站在 VPN 防火墙内网，则此选项为控制外部对此服务器上传数据时的带宽控制，例如网吧很多都有架设游戏服务器，若外部要来做此游戏服务器做数据升级时，可以用此控制做带宽管理，才不会影响内部使用者上网打游戏。 |
| 保证带宽 & 最大可用带宽：(Kbit/Sec) | 保证带宽：此为限制或保证此条规则的最小可使用带宽。<br><br>最大可用带宽：此为限制此条规则的最大可使用带宽，也就是最大不会超过此设置值。<br><br>请注意！这里填入的数值单位是 kbit，有些应用软件显示下载/上传速度单位为 KB，两个数值之间的换算方式为 1KB=8kbit。 |
| 管制时间： | 选择"所有时间"，此 QoS 设置在所有时间都有效果，如果选择"从____:____到____:____"填入时间段（24 小时记时制，例如 19：00 到 24：00），以及勾选"每天/周日/周一/周二/周三/周四/周五/周六"的某一天或者几天，其 QoS 设置只在所勾选设置的特定时间段内有效。 |

带宽分配方式： 此范围每一 IP 地址独享此设置带宽：

若选择此规则的话，其表示每一个 IP 或这一段服务端口都可以有此保证带宽到最大可用带宽)带宽范围，例如若是针对每台计算机 (IP 地址)做的规则设置，则每台计算机(IP 地址)都可以有这么大的带宽。

此范围所有 IP 地址共享此设置带宽：

若选择此规则的话，其表示所有 IP 或此服务端口共享这段(保证带宽到最大可用带宽)带宽范围。

请注意！当您选择带宽的共享方式时，要留意实际应用的情况，以避免选择不恰当的方式而造成带宽太小无法正常使用网络。例如，内网多人使用 FTP 做文件下载，若是您希望 FTP 不会占用掉大部分的带宽，您就可以选择共享带宽，不论内网有多少人使用 FTP 做文件下载，总和所占用的带宽是固定的。

激活： 启用此规则。

增加到对应列表： 增加此条规则到列表。

上移 &下移： 由于 QoS 的每条规则执行的优先级为由列表的最下面那条往上执行，也就是越后面设置的规则会优先执行，所以您可以自行调整每条规则先后执行顺序。通常将要限制带宽的服务端口移至最下方如 BT，e-mule 等，然后将针对限制 IP 带宽的规则往上移。

删所选中的项目： 删除在服务列表里所选择的项目内容。

显示开启表： 可以显示出您所有在带宽管理设置的规则，并可直接点击"编辑"做修改（见表后详解）。

确定： 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。

取消： 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

显示开启表：

点击左下方的"显示开启表"按钮，会出现以下的对话窗口。您可以选择以"规则"来显示已设置的规则，或是以"接口位置"来显示已设置的规则。点击"刷新"可以重新显示窗口，点击"关闭"将结束这个对话窗口。可直接点击"编辑"做修改。





◉ 规则 ○ 接口位置 刷新 关闭

| 服务端口 | IP地址 | 目的 | 保证带宽 (Kbit/sec) | 最大可用带宽 (Kbit/sec) | 带宽分配方式 | 激活 | 接口位置 | 编辑 |
|---|---|---|---|---|---|---|---|---|

范例一：若希望内网去做 ftp 下载都只能共同使用 50kbit 下载带宽要如何设置?

如以下范例所示设置规则，接口位置勾选广域网 1、2、3、4，服务端选择" FTP[TCP /21~21"，在 IP 地址填入 0.0.0.0 到 0(表示所有的地址)，目的选择下载。最小带宽填入 2 kbit/sec，表示 FTP 下载保证有 2kbit/sec 的带宽。最大带宽填入 50kbit/sec，表示 FTP 下载最多只能使用到 50kbit/sec 的带宽。带宽共享方式选择"此 IP 地址共享此设置带宽"，如此不论内网有多少人使用 FTP，所有 FTP 下载的带宽总和最多只能使用 50kbit/sec。勾选激活，最后点击"新增"即可将此规则加入。

## QoS带宽管理

控制类型： ◉ 带宽控制 ○ 优先级

接口位置： ☑ 广域网1 ☑ 广域网2 ☑ 广域网3 ☑ 广域网4

服务端口： FTP [TCP/21~21]

服务端口新增或删除表

IP地址 ： 0 . 0 . 0 . 0 到 0

目的： 上传

保证带宽： 2 Kbit/sec 最大可用带宽： 50 Kbit/sec

带宽分配方式： ○ 此范围每一IP地址独享此设定带宽. ◉ 此范围所有IP地址共享此设定带宽.

激活： ☑

上移 更新特殊应用软件 下移

FTP [TCP/21~21]->0.0.0.0~0(上传)=>2~50Kbit/sec->WAN1, 2, 3, 4

删除选中的项目 新增

范例二：若希望内网所有 IP 每人最大下载使用带宽只能有 512Kbit，需要一个 IP 一个 IP 设置吗?






不需要一个 IP 一个 IP 设置。如以下范例所示设置规则，接口位置勾选广域网 1、2、3、4，服务端选择"No Check Port[TCP&UDP /0~0"，在 IP 地址填入 192.168.1.2 到 254(要作限制的地址范围)，目的选择下载。最小带宽填入 2 kbit/sec，表示每个 IP 保证有 2kbit/sec 的带宽。最大带宽填入 512kbit/sec，表示每个 IP 最多只能使用到 512kbit/sec 的带宽。带宽共享方式选择"此范围每一 IP 地址最大及最小可用带宽"，如此每一个 IP 最小一定有 2kbit/sec 的保证。勾选激活，最后点击"新增"即可将此规则加入。

## QoS带宽管理

控制类型： ⦿ 带宽控制 ○ 优先级

接口位置： ☑ 广域网1 ☑ 广域网2 ☑ 广域网3 ☑ 广域网4

服务端口： Not Check Port[TCP&UDP/0~0]

服务端口新增或删除表

IP地址 : 192 . 168 . 1 . 2 到 254

目的： 下载

保证带宽： 2 Kbit/sec 最大可用带宽： 512 Kbit/sec

带宽分配方式： ⦿ 此范围每一IP地址独享此设定带宽. ○ 此范围所有IP地址共享此设定带宽.

激活： ☑

上移 更新特殊应用软件 下移

Not Check Port[TCP&UDP/0~0]->192.168.1.2~254(下载)=>2~512Kbit/sec->WAN1, 2, 3, 4

删除选中的项目 新增

范例三：若希望内网所有 IP192.168.1.100-150 每人最大下载使用带宽只能有 1M，但当使用 ftp 下载时都只能共享 512Kbit 时要如何设置?

如以下范例所示设置两条规则，第一条规则接口位置勾选广域网 1、2、3、4，服务端选择"No Check Port[TCP&UDP /0~0"，在 IP 地址填入 192.168.1.100 到 150(要作限制的地址范围)，目的选择下载。最小带宽填入 2 kbit/sec，表示每个 IP 保证有 2kbit/sec 的带宽。最大带宽填入 1024kbit/sec，表示每个 IP 最多只能使用到 1M/sec 的带宽。带宽共享方式选择"此范围每一 IP 地址最大及最小可用带宽"，如此每一个 IP 最小一定有 2kbit/sec 的保证。勾选激活，最后点击"新增"即可将此规则加入。





第二条规则接口位置勾选广域网 1、2、3、4，服务端选择"FTP[TCP/21~21"，在 IP 地址填入 0.0.0.0 到 0(表示所有的地址)，目的选择下载。最小带宽填入 2 kbit/sec，表示 FTP 下载保证有 2kbit/sec 的带宽。最大带宽填入 512kbit/sec，表示 FTP 下载最多只能使用到 512kbit/sec 的带宽。带宽共享方式选择"此 IP 地址共享此设置带宽"，如此不论内网有多少人使用 FTP，所有 FTP 下载的带宽总和最多只能使用 50kbit/sec。勾选激活，最后点击"新增"即可将此规则加入。

请注意！QoS 带宽管理的执行顺序为由列表最下面那一条往上做执行动作，所以要将先执行的规则往最下面移。以这个范例来说，先执行 FTP 的共享带宽，在执行每个 IP 的保证以及最大可用带宽。因此若是内网有人使用 FTP 下载，就会先受到第一条规则的限制，最大只能用到 512kbit/sec。若是将规则反过来，将上述的第一条规则移到最下方来先执行，则每个 IP 最大可用到 1M 的带宽，此时用 FTP 下载也就可以用到 1M 的带宽，那么后执行的 FTP 带宽限制在 512kbit 就不会执行，也就没有意义了！

## QoS带宽管理

**控制类型：** ⦿ **带宽控制** ○ **优先级**

接口位置：☑ 广域网1 ☑ 广域网2 ☑ 广域网3 ☑ 广域网4

服务端口：FTP [TCP/21~21]

服务端口新增或删除表

IP地址：0 . 0 . 0 . 0 到 0

目的：下载

保证带宽：2 Kbit/sec 最大可用带宽：512 Kbit/sec

带宽分配方式：○ 此范围每一IP地址独享此设定带宽.
⦿ 此范围所有IP地址共享此设定带宽.

激活：☑

上移 更新特殊应用软件 下移

Not Check Port[TCP&UDP/0~0]->192.168.1.100~150(下载)=>2~1024Kbit/sec->WAN1, 2, 3, 4
FTP [TCP/21~21]->0.0.0.0~0(下载)=>2~512Kbit/sec->WAN1, 2, 3, 4

删除选中的项目 新增

优先级- 依优先级做管理：

优先级顾名思义就是可以将您选定想要的服务做先后顺序的调配，也就是可以直接选择服务端口将其优先

级做一分配。

VPN 防火墙会将带宽做 60%(最高)、10%(最低)的带宽分配，也就是若您将 80 端口选择为高级，那么 VPN 防火墙只要遇到 80 端口的数据包就会给予 60%的带宽出去，若您将 FTP 端口 21 设置为低级，那当有人使用 Port 21 时，VPN 防火墙只会给它 10%的带宽使用，其余未做分配的服务端就使用 30%带宽。

## QoS带宽管理

控制类型： ○ 带宽控制 ⦿ 优先级

接口位置： ☐ 广域网1 ☐ 广域网2 ☐ 广域网3 ☐ 广域网4

服务端口： DNS [UDP/53~53]

服务端口新增或删除表

目的： 上传

优先级： 高级

激活： ☐

增加到对应列表

删除选中的项目

接口位置： 勾选此条选择优先权的设置要控制在哪条 WAN 执行。

服务端口： 在此选择此条优先权所要设置的服务端口为哪个 要针对譬如 FTP 上传或下载，则选择 FTP Port21~21，可参考下拉菜单服务号码默认列表。

| | |
|---|---|
| 目的： | 上传： 指针对此服务端口的上传做优先权控制。<br>下载： 指针对此服务端口的下载做优先权控制。<br>虚拟服务器上传(Server in LAN，上传)：若您有架设对外的 Server 网站在 VPN 防火墙内部，则此选项为控制外部访问此 Server 的带宽控制。<br>虚拟服务器下载(Server in LAN，下载)：若您有架设网站在 VPN 防火墙内网，则此选项为控制外部对此服务器上传数据时的带宽控制，例如网吧很多都有架设游戏服务器，若外部要来做此游戏服务器做数据升级时，可以用此控制做带宽管理，才不会影响内部使用者上网打游戏。 |
| 优先级： | 高级： 此为保证 60%的带宽给此服务端口使用。<br>低级： 此为只给 10%的带宽给此服务端口使用。 |
| 激活： | 启用此规则。 |
| 增加到对应列表： | 增加此条规则到列表。 |
| 删除所选中的项目： | 删除所选择在服务列表里的项目内容。 |
| 显示开启表： | 可以显示出您所有在优先权设置的规则，并可直接点击"编辑"做修改。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |






## 8.2 会话数管控

会话数管控可以控制内网的计算器最多能同时建立的会话数。这个功能对网管人员在控制内网使用 P2P 软件如 BT、迅雷、emule 等会造成大量发出会话数的软件提供了非常有效的管理。设置恰当的容许会话数可以有效控制 P2P 软件时所能产生的会话数，相对也使带宽使用量达到一定的限制。

另外，若计算机中了类似冲击波的病毒而产生大量对外发联机请求时，也可以达到抑制作用。

会话数管制设置以及时间管制：

### 会话数管理

| | |
|---|---|
| ◉ 关闭 | |
| ○ 单一IP最大可使用的会话数不可超过 [200] | |
| ○ 当单一个IP会话数到达 [200] , | ◉ 在 [5] 分钟内阻止此IP建立新会话 |
| | ○ 在 [5] 分钟内封锁此IP所有会话 |

### 生效时间

| | |
|---|---|
| 管制时间为 [所有时间] | [0] : [0] 到 [0] : [0] (时间格式:24小时制) |
| ☐ 每天 | ☐ 周日 ☐ 周一 ☐ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六 |

| | |
|---|---|
| 关闭： | 不使用此会话数管控功能。 |
| 单一 IP 最大可使用的会话数不可超过： | 此选项为限制每一台内网的计算机最大可建立的对外会话数，当用户计算机使用会话数到达此限制值时，要建立新的会话必须等到之前的会话结束后才能再建立。例如，当用户使用 BT 或 P2P 等下载时且会话数超过此设置值后，当用户又要再开其它服务时会无法使用，除非将使用中的 BT 或 P2P 软件关闭。 |
| 当单一个 IP 会话数到达： | 在____分钟内阻止此 IP 建立新会话：此选项为当客户端计算机使用会话数到达您的设置数值时，此用户在 5 分钟之内将不能再增加新会话，就算旧会话已经结束，也必须等到设置时间过后才能再建立新的会话。<br>在____分钟内封锁此 IP 所有会话：此选项为当客户端计算机使用的会话数到达您的设置数值时，此用户正在使用的所有会话都将被清除，且在 5 分钟之内将不能建立任何会话(不能上网)，必须等到设置时间过后才能再建立新的会话。 |





生效时间设置： 选择"所有时间"，此会话数管制设置在所有时间都有效果，如果选择"从___:___到___:___"填入时间段（24 小时记时制，例如 19：00 到 24：00）， 以及勾选"每天/周日/周一/周二/周三/周四/周五/周六"的某一天或者几天，其设置在所勾选设置的特定时间段内有效。

确定： 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。

取消： 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

不受限制的服务或 IP 地址

当有的用户以及 IP（比如公司管理层等），或者是特定需要不受限制的服务（公司财务数据的传输，邮件的传输等），管理人员可以设置这些服务或者 IP 不受联机管制。

### 不受限制的服务端口或IP地址

服务端口： 所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

IP地址 : 10 . 10 . 10 . 0 到 0

激活：

增加到对应列表

删除选中的项目

确定 取消

服务端口： 选择不受限制的服务端口。

IP 地址： 输入不受限制的 IP 地址范围，或者选择不受限制的 IP 群组。

激活： 启用此规则。

增加到对应列表： 将添加的规则增加到列表中。

删除选中的项目： 选择列表中的规则，删除选中的规则。

| | |
|---|---|
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |






## 8.3 动态智能带宽管理（Smart QoS）

无需网管进行设置的智能型带宽管理 Smart QoS 功能，自动压抑占用带宽用户，来解决内网 QoS 管理简化网管的管理工作。

☑ 激活动态智能QoS

当任一广域网带宽使用率到达 60 %时，激活智能QoS(此值为0表示永久激活)

内网IP在所有广域网最大容忍上传带宽：500 Kbit/sec

内网IP在所有广域网最大容忍下载带宽：1000 Kbit/sec

当任一IP使用超过上述设定上传或下载带宽时，此IP则使用下列指定频宽

上传带宽 (广域网1：300 Kbit/sec 广域网2：300 Kbit/sec
广域网3：300 Kbit/sec 广域网4：300 Kbit/sec)

下载带宽 (广域网1：300 Kbit/sec 广域网2：300 Kbit/sec
广域网3：300 Kbit/sec 广域网4：300 Kbit/sec)

☐ 激活二次惩罚

显示惩罚列表

| | |
|---|---|
| 激活动态智能 QoS: | 勾选激活动态智能 QoS。 |
| 当任一广域网带宽使用率到达____%时，激活智能 QoS | 当带宽使用率到达实际带宽的一个%比时，将启动活智能 QoS，您可输入需要的数值，系统默认是 60%。 |
| 内网 IP 在所有广域网最大容忍上传带宽 ： | 填入内网 IP 上行最大容忍使用带宽。 |
| 内网 IP 在所有广域网最大容忍下载带宽 ： | 填入内网 IP 下载最大容忍使用带宽。 |
| 当任一 IP 使用超过上述设置上传或下载带宽时，此 IP 则使用下列指定带宽： | 当任一 IP 使用超过上述设置上传或下载带宽时，就实行惩罚措施，并以各个广域网络的上传 / 下载分别设置，惩罚后允许使用的带宽是多少 |
| 激活二次性惩罚： | 点击勾选"激活二次性惩罚："后，VPN 防火墙内部设置好二次惩罚条件，当内部网络上网用户上网过程中的上传与下载达到内部条件将执行二次惩罚。 |
| 显示处罚列表： | 点击后，在弹出的对话框中将会显示 VPN 防火墙罚中的 IP，上行限制中，下载限制中以及二次惩罚信息。 |





管制时间：

选择"所有时间"，此 QoS 设置在所有时间都有效果，如果选择"从___:___到___:___"填入时间段（24 小时记时制，例如 19：00 到 24：00）， 以及勾选"每天/周日/周一/周二/周三/周四/周五/周六"的某一天或者几天，其 QoS 设置在所勾选设置的特定时间段内有效。

# 九、防火墙设置

本章节介绍防火墙设置的选项，以及网络存取控制的设置，保证网络的安全性。

## 9.1 基本设置

从防火墙功能的一般设置选项当中，您可以控制开启或是关闭这些选项功能。出厂默认值是将防火墙开启，并关闭不必要的响应。

| | |
|---|---|
| 防火墙： | ⦿ 激活 ○ 关闭 |
| SPI数据包检测： | ⦿ 激活 ○ 关闭 |
| 防止DoS攻击功能： | ⦿ 激活 ○ 关闭 高级设定 |
| 阻止广域网回应功能： | ○ 激活 ⦿ 关闭 |
| 远程管理功能： | ⦿ 激活 ○ 关闭 端口：80 |
| 允许Multicast组播穿透： | ○ 激活 ⦿ 关闭 |
| 防止ARP病毒攻击： | ○ 激活 ⦿ 关闭<br>每秒主动发送 20 笔ARP封包 |

### 禁止特殊应用

| | |
|---|---|
| 阻挡： | ☐ Java |
| | ☐ Cookies |
| | ☐ ActiveX |
| | ☐ Access to HTTP Proxy Servers |

☐ 不受限制的信任域名

### 一指键

| | |
|---|---|
| 阻挡： | ☐ MSN |
| | ☐ Skype |
| | ☐ QQ 不受限制的QQ号码 |
| | ☐ BT |

| | |
|---|---|
| 不受限制的IP地址： | ☐ 192 . 168 . 0 . 0 到 254 |
| | ☐ 192 . 168 . 0 . 0 到 254 |
| | ☐ 192 . 168 . 0 . 0 到 254 |
| | ☐ 192 . 168 . 0 . 0 到 254 |
| | ☐ 192 . 168 . 0 . 0 到 254 |





| | |
|---|---|
| 防火墙功能： | 此为选择开启或关闭防火墙功能。默认激活。 |
| SPI 数据包检测: | 此为数据包主动侦测检验技术，防火墙主要运行在网络层，但是通过执行对每个连结的动态检验，也拥有应用程序的警示功能。同时，数据包检验型防火墙可以拒绝非标准的通讯协议所使用的连结。默认激活。 |
| 防止 DoS 攻击功能: | 此为保护 DoS 攻击，如 SYN Flooding， Smurf， LAND， Ping of Death， IP Spoofing 等。默认激活。 |
| 阻止广域网响应功能: | 若是选择激活的话，则 VPN 防火墙 会关闭对外的 ICMP 与不正常联机的数据包响应，所以若是您从外部去 ping 此台 VPN 防火墙的 WAN IP 是无法 ping 通的，默认值为开启拒绝对外响应的功能。 |
| 远程管理功能: | 远程管理功能，若您要通过远程网络 直接联机进入 VPN 防火墙的设置窗口，必需将此功能开启，并于远程于浏览器网址填入 VPN 防火墙的外部合法 IP 地址(WAN IP)，并加上默认可修改的控制端口(默认为 80，可更改)。 |
| 允许 Multicast 组播穿透： | 网络上有许多影音串流媒体，使用广播方式可以让客户端接收此类数据包讯息格式。默认为关闭 |
| 防止 ARP 病毒攻击： | 此功能为防止内网遭受 ARP 欺骗攻击而造成计算机无法上网，此 ARP 病毒欺骗大多在网吧环境发生，会让所有上网计算机一瞬间掉线或部份计算机无法上网。开启此功能可以避免此种病毒攻击。 |






高级设置

| 数据包类型 | 广域网阀值设定 | | | 局域网阀值设定 | | |
|---|---|---|---|---|---|---|
| ☑ TCP_SYN_Flooding | 所有数据包阀值 | 15000 | Packets/sec | 所有数据包阀值 | 15000 | Packets/sec |
| | | | | 单一目的IP的数据包门阀值 | 0 | Packets/sec |
| | 单一IP的数据包阀值 | 2000 | Packets/sec | 单一来源IP的数据包门阀值 | 2000 | Packets/sec |
| | 达到阀值便阻挡该IP | 5 | 分钟 | 达到阀值便阻挡该IP | 5 | 分钟 |
| ☑ UDP_Flooding | 所有数据包阀值 | 15000 | Packets/sec | 所有数据包阀值 | 15000 | Packets/sec |
| | | | | 单一目的IP的数据包门阀值 | 0 | Packets/sec |
| | 单一IP的数据包阀值 | 2000 | Packets/sec | 单一来源IP的数据包门阀值 | 2000 | Packets/sec |
| | 达到阀值便阻挡该IP | 5 | 分钟 | 达到阀值便阻挡该IP | 5 | 分钟 |
| ☑ ICMP_Flooding | 所有数据包阀值 | 200 | Packets/sec | 所有数据包阀值 | 200 | Packets/sec |
| | | | | 单一目的IP的数据包门阀值 | 0 | Packets/sec |
| | 单一IP的数据包阀值 | 50 | Packets/sec | 单一来源IP的数据包门阀值 | 50 | Packets/sec |
| | 达到阀值便阻挡该IP | 5 | 分钟 | 达到阀值便阻挡该IP | 5 | 分钟 |
| ☐ 不受限制的来源IP地址 | 1. IP地址 | __.__.__.__ 到 __ | | | | |
| | 2. IP地址 | __.__.__.__ 到 __ | | | | |
| ☐ 不受限制的目的IP地址 | 1. __.__.__.__ | | | | | |
| | 2. __.__.__.__ | | | | | |
| | 3. __.__.__.__ | | | | | |
| | 4. __.__.__.__ | | | | | |
| | 5. __.__.__.__ | | | | | |

数据包类型：VPN 防火墙提供三种数据数据包传输类型，包括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood。

广域网限定值设置：防止来自外部网络的攻击。设置"所有数据包限定值"（即外部攻击的所有数据包数据），当其达到一个最大值（默认 15000pakets/Sec），VPN 防火墙将只允许通过所设置最大值的数据包数。

当单一 IP 的数据包限定值（外部单一一个 IP 地址攻击的数据包数据）达到一个最大值（默认 2000pakets/Sec），就会阻挡此 IP 上网 5 分钟（默认是 5 分钟），禁止其访问服务器，限制其流量和连接数，从而有效保证网络的安全。这里您可以根据需要调整你的限定值以及阻挡时间来达到对外网攻击的有效防护，建议其限定值从大到小来调节，避免限定值过小影响正常网络的运行。

局域网限定值设置：防止来自内部网络的攻击。同样，当所有数据包限定值（即外部攻击的所有数据包数据）达到一个最大值（默认 15000pakets/Sec），VPN 防火墙将只允许通过所设置最大值的数据包数。

当单一数据包阀值（内部单一一个 IP 地址攻击的数据包数据）达到一个最大值（默认 2000pakets/Sec），就会阻挡此 IP 上网 5 分钟（默认是 5 分钟），禁止其访问服务器，限制其流量和连接数，从而有效保证网络的安全。您可以根据需要调整你的阀值以及阻挡时间来达到对内网攻击






不受限制的来源IP地址： 输入不要被 DOS 防御设置限定值所限制的区域网来源 IP 地址或是范围

不受限制的目的IP地址： 输入不要被 DOS 防御设置限定值所限制的目的 IP 地址

(从区域网发出的数据包)

显示被阻挡的 IP：




显示被 DOS 防御功能所阻挡的 IP 地址，以及该 IP 地址还剩余多少时间解除阻挡

禁止特殊应用： VPN 防火墙支持封锁下列几种的方式连结：Java，Cookies，Active X，HTTP 代理服务器存取。

不受限制的信任域名: 若启动这项功能，使用者可以将信任的网站或者 IP 地址加入可信任的网域中，则 VPN 防火墙就不会去阻挡可信任网域的网页中所带有的 Java/ActiveX/Cookies 等项目。

确定: 点击此按钮"确定"即会存储刚才所变动的修改设置内容参数。

取消: 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于"确定"存储动作之前才会有效。





9.2 阻挡特定服务（一指键）

VPN 防火墙提供一指封特定的服务功能，可以通过设置将特殊服务 MSN、Skype、QQ、BT 下载这些服务挡住，以方便用户的管理设置。

如下图可以看出 MSN 服务被关闭，内部网络 192.168.1.2～100 的 IP 则设为例外允许的 IP 范围，仍将提供 MSN 及时信息服务功能，您可以按照需要对内网 IP 的这几个服务做挡定设置。

**一指键**

| | |
|---|---|
| 阻挡： | ☐ MSN |
| | ☐ Skype |
| | ☐ QQ 不受限制的QQ号码 |
| | ☐ BT |

| | |
|---|---|
| 不受限制的IP地址： | ☑ 192 . 168 . 1 . 2 到 100 |
| | ☐ 192 . 168 . 0 . 0 到 254 |
| | ☐ 192 . 168 . 0 . 0 到 254 |
| | ☐ 192 . 168 . 0 . 0 到 254 |
| | ☐ 192 . 168 . 0 . 0 到 254 |

另外，若激活一键封 QQ，也可以针对某些 QQ 号码能够不受封锁做设置，按下”不受限制的 QQ 号码”，跳出以下窗口即可将不受封锁限制的 QQ 号码输入，增加到下方清单以内：





| | |
|---|---|
| 用户名： | 输入能识别此 QQ 号码的信息，例如 Qno Sales。 |
| 不受限制的 QQ 号码： | 输入不受限制的 QQ 号码。 |
| 增加到对应列表： | 将添加的规则增加到列表中。 |
| 删除选中的项目： | 选择列表中的规则，删除选中的规则。 |

## 9.3 访问规则设置

VPN 防火墙设计有简而易懂的网络存取规则条例工具，管理者可以用来对不同的使用者设置不同的存取规则条件，来管理使用者对网络的存取权限。存取规则可以依据不同的条件来过滤，例如可以设置数据包要管制的进出方向是从内部到外部还是从外部到内部，或是设置以使 IP 地址、目地端 IP 地址、IP 通讯协议状态等条件来做管制，管理者可以依照实际的需求调性设置。

### 9.3.1 默认管制规则

管理者定订的网络存取规则条例，可以选择关闭或是允许来调整使用者对网络的存取。以下就针对 VPN 防火墙的网络存取规则条例做一说明：

VPN 防火墙默认的网络存取规则条例：

*从 LAN 端到 WAN 端的所有数据包可以通过-All traffic from the LAN to the WAN is allowed

*从 WAN 端到 LAN 端的所有数据包不可以通过-All traffic from the WAN to the LAN is denied

*从 LAN 端到 DMZ 端的所有数据包不可以通过-All traffic from the LAN to the DMZ is denied

*从 DMZ 端到 LAN 端的所有数据包不可以通过-All traffic from the DMZ to the LAN is denied

*从 WAN 端到 DMZ 端的所有数据包不可以通过-All traffic from the WAN to the DMZ is denied

*从 DMZ 端到 WAN 端的所有数据包不可以通过-All traffic from the DMZ to the WAN is denied

管理者可以自定存取规则并且超越 VPN 防火墙的默认存取条件规则，但是以下的四种额外服务项目为永远开启，不受其它自定规则所影响：

* HTTP 的服务从 LAN 端到 VPN 防火墙 默认为开启的 (为了管理 VPN 防火墙使用)。

* DHCP 的服务从 LAN 端到 VPN 防火墙 默认为开启的 (为了从 VPN 防火墙自动取得 IP 地址使用)。

* DNS 的服务从 LAN 端到 VPN 防火墙 默认为开启的 (为了解析 DNS 服务使用)。

* Ping 的服务从 LAN 端到 VPN 防火墙 默认为开启的 ( 为了连通测试 VPN 防火墙使用)。





跳到 1 / 2 页　　每页显示 5 笔　　下一页>>

| 优先级 | 激活 | 管制动作 | 服务端口 | 接口位置 | 来源IP地址 | 目的IP地址 | 管制时间 | 日 | 编辑 | 删除 |
|---|---|---|---|---|---|---|---|---|---|---|
| | ☑ | 允许 | 所有端口 [*] | 局域网 | 任何的 | 任何的 | 所有时间 | | | |
| | ☑ | 关闭 | 所有端口 [*] | 广域网1 | 任何的 | 任何的 | 所有时间 | | | |
| | ☑ | 关闭 | 所有端口 [*] | 广域网2 | 任何的 | 任何的 | 所有时间 | | | |
| | ☑ | 关闭 | 所有端口 [*] | 广域网3 | 任何的 | 任何的 | 所有时间 | | | |
| | ☑ | 关闭 | 所有端口 [*] | 广域网4 | 任何的 | 任何的 | 所有时间 | | | |

添加新规则　恢复出厂默认值

除了默认规则以外， 所有的网络存取规则都会显示于此规则列表中，您可以自己选择高低优先权于每一个网络存取规则项目中。VPN 防火墙在做规则确认时是依照优先权 1-2-3...。依序做规则判断，所以优先权是让您在做存取规则的设置规划中必须要考虑的，以避免您想开启或关闭的功能失效。

编辑：　可以设置网络存取规则项目。

垃圾桶图像：　可以删除网络存取规则项目。

添加新规则：　新增新的网络存取规则按钮可以新增一项新的存取规则。

恢复出厂默认值：　可以恢复到出厂原有默认存取规则项目并删除所有的自定规则内容。





9.3.2 增加新的管制规则

## 访问规则设置

| 管制动作： | 允许 | |
|---|---|---|
| 服务端口： | 所有端口 [TCP&UDP/1~65535] | 服务端口新增或删除表 |
| 日志： | 关闭 | |
| 接口位置： | 局域网 | |
| 来源IP地址： | 单独 | . . . |
| 目的IP地址： | 单独 | . . . |

## 生效时间

| 管制时间为 所有时间 | : 到 : (时间格式:24小时制) |
|---|---|
| 每天 | 周日 周一 周二 周三 周四 周五 周六 |

返回 确定 取消

| | |
|---|---|
| 管制动作: | 允许： 允许符合此管制条例行为的数据包通过。<br>关闭： 不允许符合此管制条例行为的数据包通过。 |
| 服务端口: | 从下拉式选单中选择您所要允许或不允许的服务端口服务项目内容。 |
| 服务端口新增或删除表: | 若是您想要管制的服务端口服务内容没有存在于默认列表内的话，您可以点击右方的服务端新增或删除表来新增一个服务内容。于弹出窗口中输入一个服务名称以及通讯协议与端口，点击"新增"按钮即可新增一个管制服务项目内容。 |
| 日志: | 允许: 依据此规则发生的相关事件将在日志中记录。<br>关闭: 依据此规则发生的相关事件不会日志中记录。 |
| 接口位置: | 选择您所要允许或不允许的来源数据包接口(例如是从 LAN， WAN1，WAN2 还是任何的)，可以从下拉式选单中选择。 |
| 来源 IP 地址: | 选择来源数据包的 IP 范围(如任何的，单独或者范围)，若是选择单独是范围的话，请输入此单一或是一区段范围的 IP 地址。<br>您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设置，请参考（"7.6 IP 群组管理"说明）。 |
| 目的 IP 地址: | 选择目的端数据包的 IP 范围(如任何的，单独或者范围)，若是选择单独是范围的话，请输入此单一或是一区段范围的 IP 地址。 |
| 生效时间设置: | 您可以将此条规则依照您所需要的执行时间来做控管。例如您可以设置此 |

| | |
|---|---|
| | 规则每天上午 8：00 开始执行下午 17：00 结束，或 24 小时都执行管制。 |
| 应用此存取规则: | 选择"所有时间"表示都 24 小时都执行此规则(默认) 或是可以选择从几点到几点，以及设置是每天还是某几天做管制。 |
| ...到...： | ...到...： 此管制规则有时间限制，设置方式为 24 小时制，如 08：00 到 18：00 (早上 8 点到下午 6 点)。 |
| 管制天数: | 勾选"每天"是表示每一天的这段时间都受控管，若是只针对一星期特定星期几，可以直接选择星期。 |
| 确定: | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消: | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |

范例 1：若要将病毒端口 TCP 135-139 封锁要如何设置?

首先在服务端口新增部份加入 TCP 135-139 端口(请参考如何新增服务端口的章节)，然后进行以下的设置：

管制动作：禁止

服务端口：TCP135-139

来源接口：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

来源 IP 地址：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

目的 IP 地址：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

**访问规则设置**

| | |
|---|---|
| 管制动作: | 禁止 |
| 服务端口: | TCP[TCP/135~139] 服务端口新增或删除表 |
| 日志: | 关闭 |
| 接口位置: | 任何的 |
| 来源IP地址: | 任何的 |
| 目的IP地址: | 任何的 |

范例 2：若要禁止内网 IP 段 192.168.1.200 到 192.168.1.230 禁止访问 80 端口要如何设置?

管制动作：:禁止

服务端口：TCP 80

来源界面：局域网(此意思为封锁由内网往外网的 80 端口)

来源 IP 地址：范围 192.168.1.200 到 192.168.1.230

目的 IP 地址：任何的(此意思为封锁由 192.168.1.200 到 192.168.1.230 内网往外网任何 80 端口)

**访问规则设置**

| | | |
|---|---|---|
| 管制动作： | 禁止 | |
| 服务端口： | HTTP[TCP/80~80] | 服务端口新增或删除表 |
| 日志： | 关闭 | |
| 接口位置： | 局域网 | |
| 来源IP地址： | 范围 | 192 . 168 . 1 . 200 到 192 . 168 . 1 . 230 |
| 目的IP地址： | 任何的 | |





## 9.4 网页内容管制

VPN 防火墙的网页内容管制可支持两种模式的网页管制，一为封锁禁止访问的域名，另一个为允许访问的域名，此两种模式只能使用一种。

◉ 设定允许访问的域名
○ 设定禁止访问的域名

允许访问的域名

☐ 激活

确定 取消

封锁禁止访问的域名

此功能需将完整的域名如 www.sex.com 填入，即可封锁此网站。

○ 设定允许访问的域名
◉ 设定禁止访问的域名

禁止访问的域名

☑ 激活

域名 :

不受限制的IP地址 : . . . 到

增加到对应列表

删除选中的项目

| | |
|---|---|
| 设置禁止访问的域名: | 设置那些是受管制禁止访问的域名。 |
| 激活禁止访问的域名功能: | 开启网页管制内容项目。 |
| 域名: | 填写欲管制的网址，如 www.playboy.com。 |
| 增加到对应列表: | 点击"增加到对应表"按钮新增此一欲管制的网址。 |
| 删除选中的项目: | 可以使用鼠标点选一个或多个管制的网址，然后点击即可删除。 |

网页内容过滤(关键字)：

**网页内容过滤(关键字)**

☑ **激活**

关键字： **(仅支持英文关键字)**

不受限制的IP地址 ： . . . 到

增加到对应列表

删除选中的项目

| | |
|---|---|
| 激活网页内容过滤（关键词）功能： | 当此项功能启动后，当输入网站地址有存在"sex"关键词时，则 VPN 防火墙会将所有有"sex"的网页封锁。 |
| 关键词（仅支持英文关键词）： | 输入关键词。 |
| 增加到对应列表: | 增加此新增的服务项目内容到服务表列内。 |
| 删除选中的的项目: | 选择删除服务项目内容从服务表列内。 |
| 确定: | 点击此按钮"确定"即会存储刚才所变动的修改设置内容参数。 |
| 取消: | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于"确定" 存储动作之前才会有效。 |

允许访问的域名

此功能的目的是设置只能去访问的网址，在有些公司或学校中，会只允许员工或学生只能去哪些网站，就

可以用此功能来达成。

◉ 设定允许访问的域名
○ 设定禁止访问的域名

**允许访问的域名**

☑ 激活

域名：

增加到对应列表

删除选中的项目

| | |
|---|---|
| 激活允许访问的域名功能： | 选择打勾开启允许网址管制功能，默认为关闭。 |
| 域名: | 填写欲管制的允许网址，如 www.google.com。 |
| 增加到对应列表: | 点击此按钮新增此欲管制的允许网址。 |
| 删除选中的项目: | 可以使用鼠标点选一个或多个管制的允许网址，然后点击即可删除。 |

管制内容生效时间

当选择为"所有时间"时，表示此条规则 24 小时执行。若选择"...到..."时，此管制条例会依据所设置的生效时间去执行此条规则，如管制时间为周一到周五，早上八点到下午六点，您可以参考以下图例来管制。

**生效时间**

| | |
|---|---|
| 管制时间为 所有时间 | : 到 : (时间格式:24小时制) |
| ☐ 每天 | ☐ 周日 ☐ 周一 ☐ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六 |

所有时间： 表示此管制规则 24 小时开启。

...到...: 此管制规则有时间限制，设置方式为 24 小时制，如 08：00 到 18：00 (早上 8 点到下午 6 点)。

管制天数: 勾选"每天"是表示每一天的这段时间都受控管，若是只针对一星期特定星期几，可以直接选择星期。






# 十、VPN 虚拟专用网设置

## 10.1. VPN 虚拟专用网（VPN）




PPTP隧道数：0 条已经设定使用 30 条可用隧道

IPSec + QnoKey隧道数：0 条已经设定使用 200 条可用隧道 高级设定

IPSec VPN隧道数：0 条已经设定使用 150 条可用隧道 详细信息

**VPN 隧道状态**

0 条隧道已经激活 1 条隧道已经设定

跳到 1 / 1页 每页显示 3 笔

| No. | 帐户 | 状态 | Phase2 Encrypt/Auth/DH | 本地群組 | 远程群組 | 远程网关 | 连接控制 | 配置 |
|---|---|---|---|---|---|---|---|---|
| 1 | sdfsdf | 关闭 | DES/MD5/1 | 10.10.10.0 255.255.255.0 | 192.168.2.0 255.255.255.0 | 121.30.131.143 | N/A | 编辑 |

新增一条隧道

**VPN 群組隧道状态**

| 群組名称 | 已连机隧道 | Phase2 Encrypt/Auth/DH | 本地群組 | 远程客户端 | 客户端状态 | 连接控制 | 配置 |
|---|---|---|---|---|---|---|---|

### 10.1.1. 目前所有的 VPN 状态显示

此 VPN 状态可以显示目前有关 VPN 方面的实时状态，包含：所有的隧道数(PPTP/IPSec+QnoKey 、与 IPSec VPN 隧道数），设置参数以及 GroupVPN-VPN 群组状态等信息。

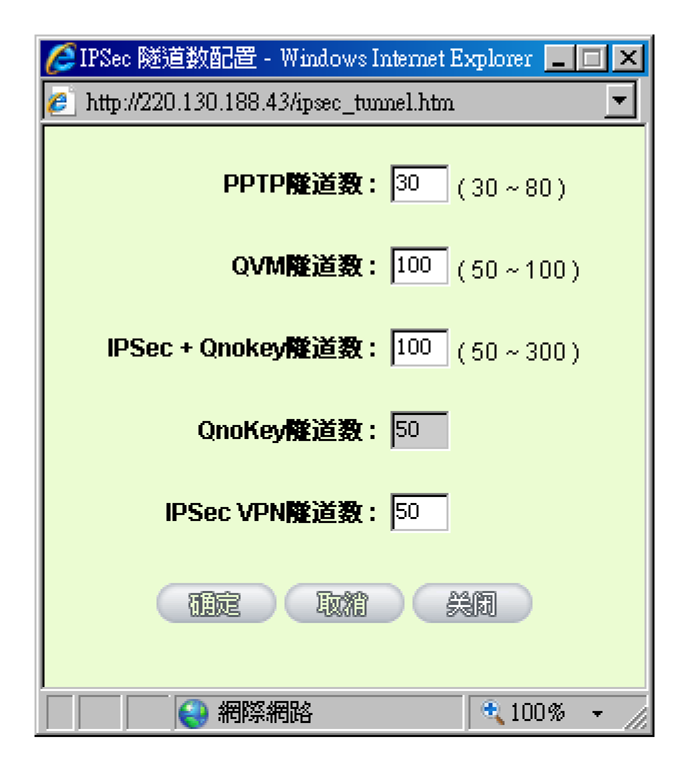




高级设置：使用者可以透过高级设置自行调整 IPSec 与 QnoKey 隧道数。

| | | | | |
|---|---|---|---|---|
| PPTP隧道数： | 0 条已经设定使用 | 30 条可用隧道 | | |
| IPSec + QnoKey隧道数： | 0 条已经设定使用 | 200 条可用隧道 | 高级设定 | |
| IPSec VPN隧道数： | 0 条已经设定使用 | 150 条可用隧道 | 详细信息 | |

此为显示目前有多少 VPN 隧道已经设置使用，还剩下多少隧道可以提供设




详细信息：按下此详细信息按钮可以显示如以下画面的目前所有 VPN 组态，让用户清楚的管理所有 VPN 连接信息。

广域网1 IP 地址: 0.0.0.0 广域网2 IP 地址: 220.130.188.40 广域网3 IP 地址: 0.0.0.0 广域网4 IP 地址: 0.0.0.0 Thu Jul 10 10:17:25 2008

| No. | 名称 | 状态 | Phase2 Encrypt/Auth/DH | 本地 群组 | 远程 群组 | 远程网关 |
|---|---|---|---|---|---|---|
| 1 | sdfsdf | 关闭 | DES/MD5/1 | 10.10.10.0 255.255.255.0 | 192.168.2.0 255.255.255.0 | 121.30.131.143 |

| 群组名称 | 已连机隧道 | Phase2 Encrypt/Auth/DH | 本地群组 | 远程客户端 | 远程网关 |
|---|---|---|---|---|---|

关闭





VPN 隧道目前状态显示（Tunnel Status）:

以下就针对"VPN 隧道状态" VPN 隧道目前状态显示做完整解说:

## VPN 隧道状态

0 条隧道已经激活　　1 条隧道已经设定

跳到 1 / 1页　　每页显示 3 笔

| No. | 帐户 | 状态 | Phase2 Encrypt/Auth/DH | 本地群组 | 远程群组 | 远程网关 | 连接控制 | 配置 |
|---|---|---|---|---|---|---|---|---|
| 1 | sdfsdf | 关闭 | DES/MD5/1 | 10.10.10.0 255.255.255.0 | 192.168.2.0 255.255.255.0 | 121.30.131.143 | N/A | 编辑 |

新增一条隧道

上一页/下一页、跳到 ___/___页、每页显示的字段

您可以按下上一页与下一页按钮跳到您想监看的 VPN 隧道画面上，或者您可以直接选择每一次所显示的页次，来监看您的所有 VPN 隧道状态，如(3，5，10，20，All)

Tunnel No.

当您设置 VPN 防火墙内建之 VPN 功能时，请选择您要设置的隧道编号

状态:

于此状态显示

已经联机成功-（Connected）

计算机名称解析失败-（Hostname Resolution Failed）

解析计算机名称（Resolving Hostname）

等待联机-（Waiting for Connection）等信息

若是用户选择手动-Manual 设置 IPSec 隧道，则此状态会显示手动-Manual 设置与没有测试此项手动设置功能状态模式

帐户名称:

目前联机 VPN 隧道连接名称，如 XXX Office，建议您若是有一个以上的隧道设置的话，务必将每一个隧道名称都设为不同，以免混淆

注意：此隧道名称若是您需要连接其它 VPN 设备(非 VPN 防火墙)时，有一些设备规定此隧道名称要与主控端为相同名称并做验证，此隧道才会顺利联机开启

Phase2 Encrypt/Auth/Group

于此显示加密(DES/3DES)以及验证(MD5/SHA1)以及群组 Group (1/2/5)等设置模式






| | |
|---|---|
| : | 若是您选择手动(Manual)设置 IPSec 的话，于此将不会显示 Phase 2 DH 群组 |
| 本地群组: | 此为显示本地区域端的 VPN 联机安全群组设置 |
| 远程群组: | 此为显示远程的 VPN 联机安全群组设置 |
| 远程网关: | 此为设置为欲与远程 VPN 设备联机的 IP 地址，请设置为远程的 VPN 防火墙的对外合法 IP 地址或是域名等 |
| 连接控制: | 可以按下"连接"按钮去验证此隧道的状态，测试结果将会更新于此状态上，在联通的情况下显示"中断"，你可以点"中断"按钮中断 VPN 连接 |
| 设置: | 设置项目包含编辑(Edit)以及删除图标<br>若您按下编辑(Edit) 按钮， 将会连接到此设置的项目当中，您可以修改其中的设置。 若您选择按下垃圾桶图标的话， 所有此隧道的设置将会被删除 |
| __条隧道已经激活、__ 条隧道已经设置 | 于此显示已有多少条隧道已被激活开启以及有多少条隧道已经被设置过 |

群组 VPN 状态显示:

若您无选择并设置群组 VPN 模式(GroupVPNs)， 此将显示出会群组 VPN 状态。

**VPN 群组隧道状态**

| 群组名称 | 已连机隧道 | Phase2 Encrypt/Auth/DH | 本地群组 | 远程客户端 | 客户端状态 | 连接控制 | 配置 |
|---|---|---|---|---|---|---|---|

| | |
|---|---|
| 群组名称: | 目前设置联机 GroupVPNs 隧道连接名称 |
| 已联机隧道: | 于此显示已经联机的 VPNGroups 隧道 |
| Phase2 Encrypt/Auth/Group: | 于此显示加密(DES/3DES)以及验证(MD5/SHA1)以及群组 Group (1/2/5)等设置模式<br>若是您选择手动(Manual)设置 IPSec 的话，于此将不会显示 Phase 2 DH 群组 |







| | |
|---|---|
| 本地群组: | 此为显示本地区域端的群组 VPN 联机安全群组设置 |
| 远程客户端: | 此为显示此群组名称远程的 VPN 联机安全群组设置 |
| 客户端状态: | 若您按下更多信息列表(Detail List) 按钮， 此将会显示更多有关信息，包含群组名称，IP 地址以及联机时间信息等 |
| 连接控制: | 可以按下连接按钮-Connect 去验证此隧道的状态，测试结果将会更新于此状态上 |
| 设置: | 如下图所示，设置项目包含编辑(Edit)以及删除图标若您按下编辑(Edit)按钮， 将会连接到此设置的项目当中，您可以修改其中的设置。 若您选择按下垃圾桶图标的话， 所有此隧道的设置将会被删除 |





10.1.2. 新增一条 VPN 隧道

VPN 防火墙支持网关对网关隧道或客户端对网关隧道。

VPN 隧道连接为 2 台 VPN 防火墙，分别通过网际网络 Internet 所组成，当您按下新增一条隧道的话， 将会直接导引到 VPN 网关对 VPN 网关的设置或客户端对 VPN 网关的设置的页面上。

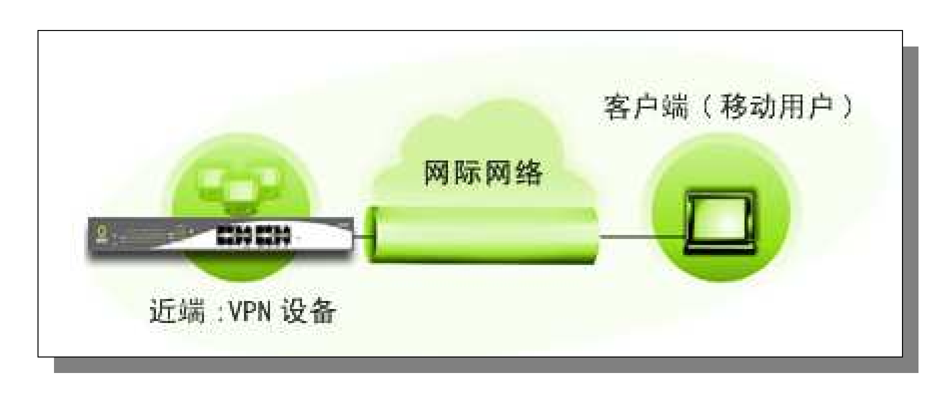
网关对网关设置（Gateway to Gateway）：

当您按下新增"新增" 的话，将会直接导引到 VPN 网关对 VPN 网关的设置页面上。




客户端对网关(Client to Gateway):

当您按下"新增" 的话， 将会直接导引到客户端对 VPN 网关的设置页面上。



10.1.2.1. 网关对网关的设置

| 隧道编号: | 1 |
| --- | --- |
| 隧道名称: | sdfsdf |
| 接口位置: | 广域网2 |
| 激活: | ☑ |

透过以下的设置说明，使用者就可以在两台 VPN 防火墙之间建立一条 VPN 隧道。

隧道编号: 当您设置 VPN 防火墙内建之 VPN 功能时，请选择您要设置的 Tunnel 隧道编号

隧道名称: 设置此隧道连接名称，如 XXX Office，建议您若是有一个以上的隧道设置的话，务必将每一个隧道名称都设为不同，以免混淆

请注意：此隧道名称若是您需要连接其它 VPN 设备(非 VPN 防火墙)时，有一些设备规定此隧道名称要与主控端为相同名称并做验证，此隧道才会顺利联机开启！。

VPN 接口地址: 您可以选择哪一个接口位置做为此 VPN 隧道的节点

激活: 勾选激活选项，将此 VPN 隧道开启。 此项目为默认为激活，当设置完成后，可以再选择是否激活隧道设置

本机用户群组设置(Local Group Setup) :

**本地用户群组配置**

| 本地网关身份类型: | 仅用IP |
| --- | --- |
| IP地址: | 0 . 0 . 0 . 0 |

| 本地安全組类型: | 子网 |
| --- | --- |
| IP地址: | 10 . 10 . 10 . 0 |
| 子网掩码: | 255 . 255 . 255 . 0 |

此项目的本地网关身分类型( Local Security Gateway Type )必须与连接远程的网关身分类型( Remote Security Gateway Type)相同。






本地网关身分类型：

本机网关认证类型，有五种操作模式项目选择，分别为:

仅用 IP

IP + Domain Name(FQDN) 认证

IP + E-mail (USER FQDN) 认证

动态 IP + Domain Name(FQDN) 认证

动态 IP + E-mail (USER FQDN) 认证

此项目的本机网关身分类型( Local Security Gateway Type )必须与连接远程的网关身分类型( Remote Security Gateway Type)相同。

(1) 仅用 IP:

若您选择仅用 IP 类型的话，只有固定填入此 IP 地址可以存取此隧道，然后 VPN 防火墙的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设置。

| 本地网关身份类型: | 仅用IP |
|---|---|
| IP地址: | 220 . 130 . 188 . 40 |

(2) IP + Domain Name(FQDN) 认证:

若您选择 IP+网域名称类型的话，请输入您所验证的网域名称以及 IP 地址然后 VPN 防火墙的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设置。

FQDN 是指主机名称以及网域名称的结合，也必须存在于 Internet 上可以查询的到，如 vpn.server.com。此 IP 地址以及网域名称必须与远程的 VPN 安全网关设置类型相同才可以正确连接。

| 本地网关身份类型: | IP + Domain Name(FQDN) 认证 |
|---|---|
| IP地址: | 220 . 130 . 188 . 40 |
| 域名: | |

(3) IP + E-mail (USER FQDN) 认证:

若您选择 IP 地址加上电子邮件类型的话， 只有固定填入此 IP 地址以及电子邮件位置可以存取此隧道，然后 VPN 防火墙的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设置。





| 本地网关身份类型: | IP + E-mail(User FQDN) 认证 |
|---|---|
| IP地址: | 220 . 130 . 188 . 40 |
| 电子邮件: | @ |

(4) 动态 IP + Domain Name(FQDN) 认证:

若是您使用动态 IP 地址连接 VPN 防火墙时， 您可以选择此类型连接 VPN， ，当远程的 VPN 网关要求与 VPN 防火墙作为 VPN 联机时，VPN 防火墙将会开始验证并响应此 VPN 隧道联机; 若您选择此类型连接 VPN，请输入网域名称即可。

| 本地网关身份类型: | 动态IP + Domain Name(FQDN) 认证 |
|---|---|
| 域名: | |

(5) 动态 IP + E-mail (USER FQDN) 认证:

若是您使用动态 IP 地址连接 VPN 防火墙时， 您可以选择此类型连接 VPN，使用者不必输入 IP 地址，当远程的 VPN 网关要求与 VPN 防火墙作为 VPN 联机时， VPN 防火墙 将会开始验证并响应此 VPN 隧道联机; 若您选择此类型连接 VPN，请输入电子邮件认证到 E-Mail 位置空格字段中即可。

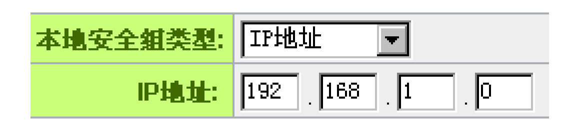
| 本地网关身份类型: | 动态IP + E-mail(User FQDN) 认证 |
|---|---|
| 电子邮件: | @ |

本地安全组类型：

此为设置本地区域端的 VPN 联机存取类型，以下有几个关于本地区域端设置的项目，请您选择并设置适当参数:

(1) IP 地址

此项目为允许此 VPN 隧道联机后，只有输入此 IP 地址的本地端计算机可以联机。



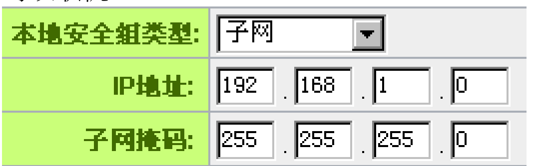

以上的设置参考为:当此 VPN 隧道联机后，于 192.168.1.0 的此 IP 地址的计算机可以联机。





(2) 子网域

此项目为允许此 VPN 隧道联机后，每一台于此网段的本地端计算机都可以联机。




以上的设置参考为:当此 VPN 隧道联机后，只有 192.168.1.0，子网掩码为 255.255.255.0 的此网段计算机可以与远程 VPN 联机。

(3) IP 地址范围

此项目为允许此 VPN 隧道联机后，只有输入此 IP 范围的本地端计算机可以联机。

| 本地安全组类型: | IP地址范围 |
|---|---|
| IP地址范围: | 192 . 168 . 1 . 0 到 254 |

以上的设置参考为:当此 VPN 隧道联机后，于 192.168.1.0~254 的此网段的 IP 地址范围的计算机可以联机。

远程用户群组设置（Remote Group Setup）：

### 远程用户群组配置

| 远程网关身份类型: | 仅用IP |
|---|---|
| IP地址 | 121 . 30 . 131 . 143 |

| 远程安全组类型: | 子网 |
|---|---|
| IP地址: | 192 . 168 . 2 . 0 |
| 子网掩码: | 255 . 255 . 255 . 0 |

此项目的远程的网关身分类型( Remote Security Gateway Type)必须与连接远程的近端本地网关身分类型( Local Security Gateway Type)相同。

远程的网关身分类型:　　远程的网关认证类型，有五种操作模式项目选择，分别为:

仅用 IP






IP + Domain Name(FQDN) 认证

IP + E-mail (USER FQDN) 认证

动态 IP + Domain Name(FQDN) 认证

动态 IP + E-mail (USER FQDN) 认证

(1) 仅用 IP:

若您选择仅用 IP 类型的话，只有固定填入此 IP 地址可以存取此隧道，




若是使用者不知道远程客户的 IP 地址，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

| 远程网关身份类型: | 仅用IP |
|---|---|
| IP by DNS Resolved | |

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

| 远程网关身份类型: | 仅用IP |
|---|---|
| IP by Multiple DNS Resolved | 1.<br>2.<br>3.<br>4. |

(2) IP + Domain Name(FQDN) 认证:

若您选择 IP+网域名称类型的话，请输入 IP 地址以及您所验证的网域名称 FQDN 是指主机名称以及网域名称的结合，使用者可以输入一个符合 FQDN 的网域名称即可。此 IP 地址以及网域名称必须与远程的 VPN 安全网关设置类型相同才可以正确连接。





| 远程网关身份类型: | IP + Domain Name(FQDN) 认证 |
|---|---|
| IP地址 | 121 . 30 . 131 . 143 |
| 域名: | |

若是使用者不知道远程的 IP 地址，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。此网域名称必须存在 Internet 上可以查询的到。并且在设置完成后在 Summary 的远程网关下面自动显示出相对应的 IP 地址

| 远程网关身份类型: | IP + Domain Name(FQDN) 认证 |
|---|---|
| IP by DNS Resolved | |
| 域名: | |

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址

| 远程网关身份类型: | IP + Domain Name(FQDN) 认证 |
|---|---|
| IP by Multiple DNS Resolved | 1.<br>2.<br>3.<br>4. |
| 域名: | |

(3) IP + E-mail(USER FQDN) 认证:

若您选择 IP 地址加上电子邮件类型的话，只有固定填入此 IP 地址以及电子邮件位置可以存取此隧道，

| 远程网关身份类型: | IP + E-mail(User FQDN) 认证 |
|---|---|
| IP地址 | 121 . 30 . 131 . 143 |
| 电子邮件: | @ |

若是使用者不知道远程客户的 IP 地址，则可以透过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

| 远程网关身份类型: | IP + E-mail(User FQDN) 认证 |
|---|---|
| IP by DNS Resolved | |
| 电子邮件: | @ |






或者也可以通过Multiple DNS Resolved 来将DNS 转成IP 地址。并且在设置完成后在Summary 的远程网关下面显示出相对应的IP 地址。

| 远程网关身份类型: | IP + E-mail (User FQDN) 认证 |
|---|---|
| IP by Multiple DNS Resolved | 1.<br>2.<br>3.<br>4. |
| 电子邮件: | @ |

(4) 动态 IP + Domain Name(FQDN) 认证:

若是您使用动态 IP 地址连接 VPN 防火墙时，您可以选择动态 IP 地址加上主机名称以及网域名称的结合。

| 远程网关身份类型: | 动态IP + Domain Name (FQDN) 认证 |
|---|---|
| 域名: | |

(5) 动态 IP + E-mail (USER FQDN) 认证:

若是您使用动态 IP 地址连接 VPN 防火墙时， 您可以选择此类型连接 VPN，当远程的 VPN 网关要求与 VPN 防火墙作为 VPN 联机时，VPN 防火墙 将会开始验证并响应此 VPN 隧道联机; 请输入电子邮件认证到 E-Mail 位置空格字段中。

| 远程网关身份类型: | 动态IP + E-mail (User FQDN) 认证 |
|---|---|
| 电子邮件: | @ |






远程安全组类型: 此为设置远程端的 VPN 联机存取类型，以下有几个关于远程端设置的项目，请您选择并设置适当参数:

(1) IP 地址

此项目为允许此 VPN 隧道联机后，只有输入此 IP 地址的本地端计算机可以联机。

| 远程安全組类型: | IP地址 |
|---|---|
| IP地址: | 192 . 168 . 2 . 1 |

以上的设置参考为:当此 VPN 隧道联机后，于 192.168.2.1 的此 IP 地址范围的计算机可以联机。

(2)子网域

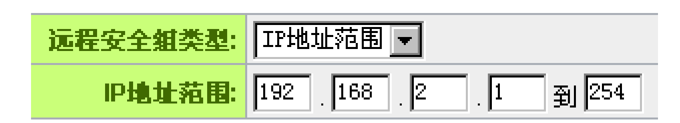
此项目为允许此 VPN 隧道联机后，每一台于此网段的本地端计算机都可以联机。




以上的设置参考为:当此 VPN 隧道联机后，只有 192.168.2.0，子网掩码为 255.255.255.0 的此网段计算机可以与远程 VPN 联机

(3)IP 地址范围

此项目为允许此 VPN 隧道联机后，只有输入此 IP 地址范围的本地端计算机可以联机




以上的设置参考为:当此 VPN 隧道联机后，只有 192.168.2.1 到 192.168.2.254 的 IP 地址范围的计算机可以联机。

IPSec Setup

若是任何加密机制存在的话，此两个 VPN 隧道的加密机制必须要相同才可以将此隧道连接，并于传输资料中加上标准的 IPSec 密钥，我们称为加密密钥 “key”。VPN 防火墙提供了以下二种加密管理模式 Key Management，分别为手动(Manual) 以及 IKE 自动加密模式- IKE with Preshared Key






(automatic)，你可以通过下拉菜单选择需要的加密模式如下图所示。

**IPSec 配置**

| | |
|---|---|
| 密钥管理协定: | 使用IKE协定 |
| 阶段1 DH协议群組: | 群組1 |
| 阶段1 加密演算法: | DES |
| 阶段1 认证演算法: | MD5 |
| 阶段1 SA有效时间: | 28800 秒 |
| 完全顺向密钥(PFS) | ☑ |
| 阶段2 DH协议群組: | 群組1 |
| 阶段2 加密演算法: | DES |
| 阶段2 认证演算法: | MD5 |
| 阶段2 SA有效时间: | 3600 秒 |
| 共用密钥: | test |

高级设定 +

密钥管理协议:

此选项设置为当您设置此 VPN 隧道使用何种加密模式以及验证模式后，必须设置一组交换密码，并请注意此参数必须与远程的交换密码参数相同;设置的方式有自动 Auto (IKE)或是手动 Manual 设置二种，于设置时请您选择其中一种设置方式即可！

### IPSec 配置

| 密钥管理协定: | 使用IKE协定 |
| --- | --- |
| 阶段1 DH协议群组: | 群組1 |
| 阶段1 加密演算法: | DES |
| 阶段1 认证演算法: | MD5 |
| 阶段1 SA有效时间: | 28800 秒 |
| 完全顺向密钥(PFS) | ☑ |
| 阶段2 DH协议群组: | 群組1 |
| 阶段2 加密演算法: | DES |
| 阶段2 认证演算法: | MD5 |
| 阶段2 SA有效时间: | 3600 秒 |
| 共用密钥: | test |

高级设定 +

使用 IKE 协定:

透过 IKE 产生共享的金钥来加密与验证远程的使用者。若将完全顺向密钥 PFS(Perfect Forward Secrecy)激活后，则会再第二阶段的 IKE 协调过程产生的第二把共同金钥做进一步加密与验证。当 PFS 激活后，透过 brute force 来撷取金钥的骇客(hacker)无法在此短时间内，进一步得到第二把金钥。

- 完全顺向密钥(Perfect Forward Secrecy)：若您将 PFS 选项勾选后，记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。
- 阶段 1/阶段 2 DH 协议群组：于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。
- 阶段 1/阶段 2 加密算法：此加密选项设置为设置此 VPN 隧道使用何种加密模式，并请注意设置此参数必须与远程的加密参数相同:DES:64-位加密模式、3DES:128-位加密模式、AES:用安全码进行信息加密的标准，它支持 128 位、192 位和 256 位的密匙。
- 阶段 1/阶段 2 认证算法：此验证选项设置为设置此 VPN 隧道使用何种验证模式，并请注意设置此参数必须与远程的验证模式参数相同:"MD5"或"SHA1"。
- 阶段 1 SA 有效时间：为此交换密码的有效时间，系统默认值为 28800 秒(8 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。
- 阶段 2 SA 有效时间：为此交换密码的有效时间，系统默认值为 3600 秒(1 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全
- 共享密钥：于 Auto (IKE) 选项中，您必须输入一组交换密码于 "Pre-shared Key" 的字段中，

在此的范例设置为 test，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 隧道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 30 个文字组合。

Manual-手动方式

IPSec 配置

| 密钥管理协定: | 手动输入 |
|---|---|
| Incoming SPI: | |
| Outgoing SPI: | |
| 加密演算法: | DES |
| 认证演算法: | MD5 |
| 加密密钥: | |
| 认证密钥: | |

若您选择手动模式 Manual 的话，此提供您自定加密密钥，而此密钥不需经过任何交握。

- 于此分成加密密钥"Encryption KEY"以及验证密钥"Authentication KEY"二种，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 隧道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 23 个文字组合。
- 另外还需要设置"Incoming SPI"的交换字符串以及"Outgoing SPI" 交换字符串，此字符串必须与远程 VPN 设备连接时相同;于此的 Incoming SPI 设置参数，您必须在远程的 VPN 设备的 Outgoing SPI 设置相同字符串，而于本地端的 Outgoing SPI 设置字符串，也必须与在远程的 VPN 设备的 Incoming SPI 设置相同字符串！

高级设置-只供给使用 IKE 协议使用

**高级设定**

- ☑ 野蛮模式
- ☐ 使用IP Header压缩协定
- ☐ 保持连接
- ☐ AH哈希算法 MD5
- ☐ 允许NetBIOS广播封包通过
- ☐ 允许掉线侦测封包穿越NAT
- ☐ 掉线侦测功能(DPD) 每隔 10 秒进行侦测

在 VPN 防火墙的进阶设置项目中，分别有 Main 以及 Aggressive（野蛮模式）模式，Main mode 是 VPN 防火墙的默认 VPN 作业模式，而且与大多数的其它 VPN 设备使用连接方式为相同。

- 野蛮模式（Aggressive Mode）：大多为远程的设备采用，如使用动态 IP 连接时，是为了加强其安全控管机制。
- 使用 IP Header 压缩协议：若选择此项目勾选，则连接的 VPN 隧道中 VPN 防火墙 支持 IP 表头形态的压缩(IP Payload compression Protocol)。
- 持续保持联机：若选择此项目勾选，则连接的 VPN 隧道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 地址的远程使用。
- AH 哈希算法：AH (Authentication Header) 验证表头数据包格式，可选择 MD5/DSHA-1。
- 允许 NetBIOS 广播数据包通过：若选择此项目勾选，则连接的 VPN 隧道中会让 NetBIOS 广播数据包通过。，有助于微软的网络邻居等连接容易，但是相对的占用此 VPN 隧道的流量就会加大！
- 允许穿越 NAT：允许 VPN 可以穿透位于 VPN 防火墙前方的 NAT 机制
- 掉线侦测功能(DPD)：若选择此项目勾选，则连接的 VPN 隧道中会定期的传送 HELLO/ACK 讯息数据包来侦测是否 VPN 隧道的两端仍有联机存在。当有一端断线则 VPN 防火墙会自动断线，然后再建立新联机。使用者可以选择每一次 DPD 讯息数据包传递的时间，默认值为 10 秒。





10.1.2.2. 客户端对网关的设置

透过以下的设置说明，管理人员就可以在客户端与 VPN 防火墙之间建立一条 VPN 隧道。

用户可以选择这一条 VPN 隧道在客户端是只供一个客户所使用(Tunnel)或者是由一群客户所使用(Group VPN)。若由一群客户所使用则可以节省个别设置远程的客户，只需设置的一条隧道供一组客户所使用，以节省设置时的麻烦。

（1） 在隧道模式（Tunnel）的情况:

◉ 隧道模式 ○ VPN群組模式

| | |
|---|---|
| 隧道编号: | 2 |
| 隧道名称: | |
| 接口位置: | 广域网1 |
| 激活: | ☑ |

隧道编号: 当您设置 VPN 防火墙内建之 VPN 功能时，请选择您要设置的 Tunnel 隧道编号。

隧道名称: 设置此隧道连接名称，如 XXX Office，建议您若是有一个以上的隧道设置的话，务必将每一个隧道名称都设为不同，以免混淆

请注意：此隧道名称若是您需要连接其它 VPN 设备时，有一些设备规定此隧道名称要与主控端为相同名称并做验证，此隧道才会顺利联机开启！。

VPN 接口地址: 您可以选择哪一个接口位置做为此 VPN 隧道的节点

激活: 勾选激活 选项，将此 VPN 隧道开启。 此项目为默认为激活，当设置完成后可以再选择是否激活隧道设置。






本机用户群组设置(Local Group Setup)

此项目的本地网关身分类型( Local Security Gateway Type )必须与连接远程的网关身分类型( Remote Security Gateway Type)相同。

本地网关身分类型：

本机网关认证类型，有五种操作模式项目选择，分别为:

仅用 IP

IP + Domain Name(FQDN) 认证

IP + E-mail (USER FQDN) 认证

动态 IP + Domain Name(FQDN) 认证

动态 IP + E-mail(USER FQDN) 认证

此项目的本地网关身分类型( Local Security Gateway Type )必须与连接远程的网关身分类型( Remote Security Gateway Type)相同。

(1) 仅用 IP:

若您选择仅用 IP 类型的话， 只有固定填入此 IP 地址可以存取此隧道，然后 VPN 防火墙的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设置。




(2) IP + Domain Name(FQDN) 认证:

若您选择 IP+网域名称类型的话，请输入您所验证的网域名称以及 IP 地址然后 VPN 防火墙的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设置。 FQDN 是指主机名称以及网域名称的结合，也必须存在于 Internet 上可以查询的到，如 vpn.server.com。此 IP 地址以及网域名称必须与远程的 VPN 安全网关设置类型相同才可以正确连接。





| 本地网关身份类型: | IP + Domain Name(FQDN) 认证 |
|---|---|
| IP地址: | 0 . 0 . 0 . 0 |
| 域名: | |

(3) IP + E-mail(USER FQDN) 认证:

若您选择 IP 地址加上电子邮件类型的话， 只有固定填入此 IP 地址以及电子邮件位置可以存取此隧道，然后 VPN 防火墙的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设置。

| 本地网关身份类型: | IP + E-mail(User FQDN) 认证 |
|---|---|
| IP地址: | 0 . 0 . 0 . 0 |
| 电子邮件: | @ |

(4) 动态 IP + Domain Name(FQDN) 认证:

若是您使用动态 IP 地址连接 VPN 防火墙时， 您可以选择此类型连接 VPN， ，当远程的 VPN 网关要求与 VPN 防火墙作为 VPN 联机时，VPN 防火墙 将会开始验证并响应此 VPN 隧道联机; 若您选择此类型连接 VPN，请输入网域名称即可。

| 本地网关身份类型: | 动态IP + Domain Name(FQDN) 认证 |
|---|---|
| 域名: | |

(5) 动态 IP + E-mail (USER FQDN) 认证:

若是您使用动态 IP 地址连接 VPN 防火墙时， 您可以选择此类型连接 VPN，使用者不必输入 IP 地址，当远程的 VPN 网关要求与 VPN 防火墙作为 VPN 联机时，VPN 防火墙 将会开始验证并响应此 VPN 隧道联机; 若您选择此类型连接 VPN，请输入电子邮件认证到 E-Mail 位置空格字段中即可。

| 本地网关身份类型: | 动态IP + E-mail(User FQDN) 认证 |
|---|---|
| 电子邮件: | @ |

本地安全组类型：

此为设置本地区域端的 VPN 联机存取类型，以下有几个关于本地区域端设置的项目，请您选择并设置适当参数:





(1)IP 地址

此项目为允许此 VPN 隧道联机后，只有输入此 IP 地址的本地端计算机可以联机。




以上的设置参考为:当此 VPN 隧道联机后，于 192.168.1.0 的此 IP 地址的计算机可以联机。

(2)子网域

此项目为允许此 VPN 隧道联机后，每一台于此网段的本地端计算机都可以联机。




以上的设置参考为:当此 VPN 隧道联机后，只有 192.168.1.0，子网掩码为 255.255.255.0 的此网段计算机可以与远程 VPN 联机。

(3)IP 地址范围

此项目为允许此 VPN 隧道联机后，只有输入此 IP 范围的本地端计算机可以联机。




以上的设置参考为:当此 VPN 隧道联机后，于 192.168.1.0~254 的此网段的 IP 地址范围的计算机可以联机。

远程用户群组设置（Remote Group Setup）:

### 远程用户群组配置

| 远程网关身份类型: | 仅用IP |
|---|---|
| IP地址 | . . . |

此项目的远程的网关身分类型( Remote Security Gateway Type)必须与连接远程的近端本地网关身分类型( Local Security Gateway Type)相同。

远程的网关认证类型: 远程的网关认证类型，有五种操作模式项目选择，分别为:

仅用 IP

IP + Domain Name(FQDN) 认证

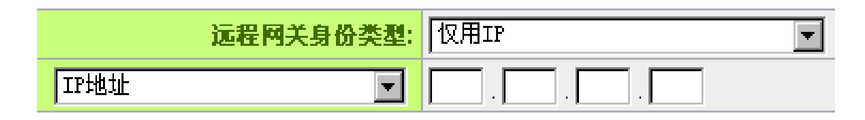
IP + E-mail (USER FQDN) 认证

动态 IP + Domain Name(FQDN) 认证

动态 IP + E-mail (USER FQDN) 认证

(1) 仅用 IP:

若您选择仅用 IP 类型的话，只有固定填入此 IP 地址可以存取此隧道，




若是使用者不知道远程客户的 IP 地址，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

| 远程网关身份类型: | 仅用IP |
|---|---|
| IP by DNS Resolved | |

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。





| 远程网关身份类型: | 仅用IP |
|---|---|
| IP by Multiple DNS Resolved | 1. <br> 2. <br> 3. <br> 4. |

(2) IP + Domain Name(FQDN) 认证:

若您选择 IP+网域名称类型的话，请输入 IP 地址以及您所验证的网域名称 FQDN 是指主机名称以及网域名称的结合，使用者可以输入一个符合 FQDN 的网域名称即可。此 IP 地址以及网域名称必须与远程的 VPN 安全网关设置类型相同才可以正确连接。

| 远程网关身份类型: | IP + Domain Name(FQDN) 认证 |
|---|---|
| IP地址 | 121 . 30 . 131 . 143 |
| 域名: | |

若是使用者不知道远程的 IP 地址，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。此网域名称必须存在 Internet 上可以查询的到。并且在设置完成后在 Summary 的远程网关下面自动显示出相对应的 IP 地址。

| 远程网关身份类型: | IP + Domain Name(FQDN) 认证 |
|---|---|
| IP by DNS Resolved | |
| 域名: | |

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

| 远程网关身份类型: | IP + Domain Name(FQDN) 认证 |
|---|---|
| IP by Multiple DNS Resolved | 1. <br> 2. <br> 3. <br> 4. |
| 域名: | |

(3) IP + E-mail (USER FQDN) 认证:

若您选择 IP 地址加上电子邮件类型的话，只有固定填入此 IP 地址以





及电子邮件位置可以存取此隧道，

| 远程网关身份类型: | IP + E-mail(User FQDN) 认证 |
|---|---|
| IP地址 | . . . |
| 电子邮件: | @ |

若是使用者不知道远程客户的 IP 地址，则可以透过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

| 远程网关身份类型: | IP + E-mail(User FQDN) 认证 |
|---|---|
| IP by DNS Resolved | |
| 电子邮件: | @ |

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

| 远程网关身份类型: | IP + E-mail(User FQDN) 认证 |
|---|---|
| IP by Multiple DNS Resolved | 1.<br>2.<br>3.<br>4. |
| 电子邮件: | @ |

(4) 动态 IP + Domain Name(FQDN) 认证:

若是您使用动态 IP 地址连接 VPN 防火墙时，您可以选择动态 IP 地址加上主机名称以及网域名称的结合。

| 远程网关身份类型: | 动态IP + Domain Name(FQDN) 认证 |
|---|---|
| 域名: | |

(5) 动态 IP + E-mail (USER FQDN) 认证:

若是您使用动态 IP 地址连接 VPN 防火墙时， 您可以选择此类型连接 VPN，当远程的 VPN 网关要求与 VPN 防火墙作为 VPN 联机时，VPN 防火墙 将会开始验证并响应此 VPN 隧道联机; 请输入电子邮件认证到 E-Mail 位置空格字段中。





| 远程网关身份类型: | 动态IP + E-mail (User FQDN) 认证 |
|---|---|
| 电子邮件: | @ |

IPSec Setup

## IPSec 配置

| 密钥管理协定: | 使用IKE协定 |
|---|---|
| 阶段1 DH协议群組: | 群組1 |
| 阶段1 加密演算法: | DES |
| 阶段1 认证演算法: | MD5 |
| 阶段1 SA有效时间: | 28800 秒 |
| 完全順向密钥(PFS) | ☑ |
| 阶段2 DH协议群組: | 群組1 |
| 阶段2 加密演算法: | DES |
| 阶段2 认证演算法: | MD5 |
| 阶段2 SA有效时间: | 3600 秒 |
| 共用密钥: | |

高级设定 +

若是任何加密机制存在的话，此两个 VPN 隧道的加密机制必须要相同才可以将此隧道连接，并于传输资料中加上标准的 IPSec 密钥，于此我们称为加密密钥 “key”。VPN 防火墙提供了以下二种加密管理模式，分别为手动(Manual ) 以及 IKE 自动加密模式- IKE with Preshared Key (automatic)如下图所示。

密钥管理协议:

此选项设置为当您设置此 VPN 隧道使用何种加密模式以及验证模式后，必须设置一组交换密码，并请注意此参数必须与远程的交换密码参数相同;设置的方式有自动 Auto (IKE)或是手动 Manual 设置二种，于设置时请您选择其中一种设置方式即可！

## IPSec 配置

| | |
|---|---|
| 密钥管理协定: | 使用IKE协定 |
| 阶段1 DH协议群组: | 群組1 |
| 阶段1 加密演算法: | DES |
| 阶段1 认证演算法: | MD5 |
| 阶段1 SA有效时间: | 28800 秒 |
| 完全顺向密钥(PFS) | ☑ |
| 阶段2 DH协议群组: | 群組1 |
| 阶段2 加密演算法: | DES |
| 阶段2 认证演算法: | MD5 |
| 阶段2 SA有效时间: | 3600 秒 |
| 共用密钥: | |

高级设定 +

使用 IKE 协定:

透过 IKE 产生共享的金钥来加密与验证远程的使用者。若将完全顺向密钥 PFS(Perfect Forward Secrecy)激活后，则会再第二阶段的 IKE 协调过程产生的第二把共同金钥做进一步加密与验证。当 PFS 激活后，透过 brute force 来撷取金钥的骇客(hacker)无法在此短时间内，进一步得到第二把金钥。

- 完全顺向密钥(Perfect Forward Secrecy)：若您将 PFS 选项勾选后，记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。
- 阶段 1/阶段 2 DH 协议群组：于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。
- 阶段 1/阶段 2 加密算法：此加密选项设置为设置此 VPN 隧道使用何种加密模式，并请注意设置此参数必须与远程的加密参数相同:DES:64-位加密模式、3DES:128-位加密模式、AES:用安全码进行信息加密的标准，它支持 128 位、192 位和 256 位的密匙。
- 阶段 1/阶段 2 认证算法：此验证选项设置为设置此 VPN 隧道使用何种验证模式，并请注意设置此参数必须与远程的验证模式参数相同:"MD5"或"SHA1"。
- 阶段 1 SA 有效时间：为此交换密码的有效时间，系统默认值为 28800 秒(8 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。
- 阶段 2 SA 有效时间：为此交换密码的有效时间，系统默认值为 3600 秒(1 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全

- 共享密钥：于 Auto (IKE) 选项中，您必须输入一组交换密码于 "Pre-shared Key" 的字段中，在此的范例设置为 test，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 隧道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 30 个文字组合。

Manual-手动方式

### IPSec 配置

| | |
|---|---|
| 密钥管理协定: | 手动输入 |
| Incoming SPI: | |
| Outgoing SPI: | |
| 加密演算法: | DES |
| 认证演算法: | MD5 |
| 加密密钥: | |
| 认证密钥: | |

若您选择手动模式 Manual 的话，此提供您自定加密密钥，而此密钥不需经过任何交握。

- 于此分成加密密钥"Encryption KEY"以及验证密钥"Authentication KEY"二种，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 隧道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 23 个文字组合。
- 另外还需要设置"Incoming SPI"的交换字符串以及"Outgoing SPI" 交换字符串，此字符串必须与远程 VPN 设备连接时相同;于此的 Incoming SPI 设置参数，您必须在远程的 VPN 设备的 Outgoing SPI 设置相同字符串，而于本地端的 Outgoing SPI 设置字符串，也必须与在远程的 VPN 设备的 Incoming SPI 设置相同字符串！






Advanced(进阶作业模式)-只供给使用自动交换密钥模式使用(IKE Preshareed Key Only)

**高级设定**

- ☑ 野蛮模式
- ☐ 使用IP Header压缩协定
- ☐ 保持连接
- ☐ AH哈希算法 MD5
- ☐ 允许NetBIOS广播封包通过
- ☐ 允许掉线侦测封包穿越NAT
- ☐ 掉线侦测功能(DPD) 每隔 10 秒进行侦测

在 VPN 防火墙 的进阶设置项目中，分别有 Main 以及 Aggressive。模式，Main mode 是 VPN 防火墙的默认 VPN 作业模式，而且与大多数的其它 VPN 设备使用连接方式为相同。

- 野蛮模式（Aggressive Mode）：大多为远程的设备采用，如使用动态 IP 连接时，是为了加强其安全控管机制。
- 使用 IP Header 压缩协定：若选择此项目勾选，则连接的 VPN 隧道中 VPN 防火墙 支持 IP 表头形态的压缩(IP Payload compression Protocol)。
- 持续保持联机：若选择此项目勾选，则连接的 VPN 隧道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 地址的远程使用。
- AH 哈希算法：AH (Authentication Header) 验证表头数据包格式，可选择 MD5/DSHA-1。
- 允许 NetBIOS 广播数据包通过：若选择此项目勾选，则连接的 VPN 隧道中会让 NetBIOS 广播数据包通过。，有助于微软的网络邻居等连接容易，但是相对的占用此 VPN 隧道的流量就会加大！
- 允许穿越 NAT：允许 VPN 可以穿透位于 VPN 防火墙前方的 NAT 机制
- 掉线侦测功能(DPD)：若选择此项目勾选，则连接的 VPN 隧道中会定期的传送 HELLO/ACK 讯息数据包来侦测是否 VPN 隧道的两端仍有联机存在。当有一端断线则 VPN 防火墙会自动断线，然后再建立新联机。使用者可以选择每一次 DPD 讯息数据包传递的时间，默认值为 10 秒。





（2） 在 Group VPN 的情况:

○ **隧道模式** ◉ **VPN群組模式**

| **群组编号:** | 1 |
|---|---|
| **群组名称:** | |
| **接口位置:** | 广域网1 |
| **激活:** | ☑ |

群组编号: 最多可以设置两组 Group VPN。

群组名称: 设置此隧道连接名称，如 XXX Office，建议您若是有一个以上的隧道设置的话，务必将每一个隧道名称都设为不同，以免混淆。

请注意：此隧道名称若是您需要连接其它 VPN 设备(非 VPN 防火墙)时，有一些设备规定此隧道名称要与主控端为相同名称并做验证，此隧道才会顺利联机开启！。

接口位置: 您可以选择哪一个接口位置做为此 VPN 隧道的节点

激活: 勾选激活 选项，将此 VPN 隧道开启。 此项目为默认为激活 Eanble，当设置完成后可以再选择是否激活隧道设置。

本机用户群组设置：

本地安全组类型: 此为设置本地区域端的 VPN 用户群组类型，以下有几个关于本地区域端设置的项目，请您选择并设置适当参数:

(1) IP 地址

此项目为允许此 VPN 隧道联机后，只有输入此 IP 地址的本地端计算机可以联机。




以上的设置参考为:当此 VPN 隧道联机后，于 192.168.1.0 的 IP 地址范围的计算机可以联机。

(2) 子网域





此项目为允许此 VPN 隧道联机后，每一台于此网段的本地端计算机都可以联机。

| 本地安全組类型: | 子网 |
|---|---|
| IP地址: | 192 . 168 . 1 . 0 |
| 子网掩码: | 255 . 255 . 255 . 0 |

以上的设置参考为:当此 VPN 隧道联机后，只有 192.168.1.0，子网掩码为 255.255.255.0 的此网段计算机可以与远程 VPN 联机。

(3) IP 地址范围

此项目为允许此 VPN 隧道联机后，只有输入此 IP 范围的本地端计算机可以联机。

| 本地安全組类型: | IP地址范围 |
|---|---|
| IP地址范围: | 192 . 168 . 1 . 0 到 254 |

以上的设置参考为:当此 VPN 隧道联机后，于 192.168.1.0~254 的此网段的 IP 地址范围的计算机可以联机。

远程用户群组设置

## 远程用户群组配置

| 远程用户认证类型: | 域名 (FQDN) |
|---|---|
| 域名: | |

远程用户认证类型: 远程客户端设置，有三种操作模式项目选择，分别为:

Domain Name(FQDN)：网域名称

E-mail Address(USER FQDN)：电子邮件名称

Microsoft XP/2000 VPN Client：微软 XP/2000 VPN 客户端

(1) Domain Name(FQDN):网域名称

若您选择网域名称类型的话，请输入您所验证的网域名称。FQDN 是指主机名称以及网域名称的结合，也必须存在于 Internet 上可以查询的到，如 vpn.Server.com。此网域名称必须与客户端的近端设置形态相同才可以正确连接。





| 远程用户认证类型: | 域名 (FQDN) |
|---|---|
| 域名: | |

(2) E-mail (USER FQDN): 电子邮件名称

若您选择电子邮件类型的话，只有固定填入此电子邮件位置可以存取此隧道。

| 远程用户认证类型: | 电子邮件 (USER FQDN) |
|---|---|
| 电子邮件: | @ |

(3) Microsoft XP/2000 VPN Client: 微软 XP/2000 VPN 客户端

若您选择微软 XP/2000 VPN 客户端形态的话，您不需要在进行额外设置。

| 远程用户认证类型: | Microsoft XP/2000 VPN客户端 |
|---|---|

IPSec Setup

若是任何加密机制存在的话，此两个 VPN 隧道的加密机制必须要相同才可以将此隧道连接，并于传输资料中加上标准的 IPSec 密钥，于此我们称为加密密钥 "key"。VPN 防火墙提供了以下二种加密管理模式，分别为手动(Manual) 以及 IKE 自动加密模式- IKE with Preshared Key (automatic)。

在选择 Group VPN 的情况之下或者是在远程网关安全角态 Remote Security Gateway Type 中使用动态位置 IP 时，Aggressive Mode 会自动激活，没有手动 Manual 模式。

密钥管理协定:

## IPSec 配置

| 密钥管理协定: | 使用IKE协定 |
|---|---|
| 阶段1 DH协议群組: | 群組1 |
| 阶段1 加密演算法: | DES |
| 阶段1 认证演算法: | MD5 |
| 阶段1 SA有效时间: | 28800 秒 |
| 完全顺向密钥(PFS) | ☑ |
| 阶段2 DH协议群組: | 群組1 |
| 阶段2 加密演算法: | DES |
| 阶段2 认证演算法: | MD5 |
| 阶段2 SA有效时间: | 3600 秒 |
| 共用密钥: | |

高級设定 +

- 完全顺向密钥(Perfect Forward Secrecy)：若您将 PFS 选项勾选后，记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。
- 阶段 1/阶段 2 DH 协议群组：于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。
- 阶段 1/阶段 2 加密算法：此加密选项设置为设置此 VPN 隧道使用何种加密模式，并请注意设置此参数必须与远程的加密参数相同:DES:64-位加密模式、3DES:128-位加密模式、AES:用安全码进行信息加密的标准，它支持 128 位、192 位和 256 位的密匙。
- 阶段 1/阶段 2 认证算法：此验证选项设置为设置此 VPN 隧道使用何种验证模式，并请注意设置此参数必须与远程的验证模式参数相同:"MD5"或"SHA1"。
- 阶段 1 SA 有效时间：为此交换密码的有效时间，系统默认值为 28800 秒(8 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。
- 阶段 2 SA 有效时间：为此交换密码的有效时间，系统默认值为 3600 秒(1 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全
- 共享密钥：于 Auto (IKE) 选项中，您必须输入一组交换密码于 "Pre-shared Key" 的字段中，在此的范例设置为 test，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 隧道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 30 个文字组合。





高级设置-只供给使用 IKE 协议使用(IKE Preshareed Key Only)

高级设定

- 野蛮模式
- 使用IP Header压缩协定
- 保持连接
- AH哈希算法 MD5
- 允许NetBIOS广播封包通过
- 允许掉线侦测封包穿越NAT
- 掉线侦测功能(DPD) 每隔 10 秒进行侦测

在 VPN 防火墙的进阶设置项目中，分别有 Main 以及 Aggressive 模式，Main mode 是 VPN 防火墙的默认 VPN 作业模式，而且与大多数的其它 VPN 设备使用连接方式为相同。

- 野蛮模式（Aggressive Mode）：大多为远程的设备采用，如使用动态 IP 连接时，是为了加强其安全控管机制。
- 使用 IP Header 压缩协定：若选择此项目勾选，则连接的 VPN 隧道中 VPN 防火墙支持 IP 表头形态的压缩(IP Payload compression Protocol)。
- 持续保持联机：若选择此项目勾选，则连接的 VPN 隧道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 地址的远程使用。
- AH 哈希算法：AH (Authentication Header) 验证表头数据包格式，可选择 MD5/DSHA-1。
- 允许 NetBIOS 广播数据包通过：若选择此项目勾选，则连接的 VPN 隧道中会让 NetBIOS 广播数据包通过。，有助于微软的网络邻居等连接容易，但是相对的占用此 VPN 隧道的流量就会加大！
- 允许穿越 NAT：允许 VPN 可以穿透位于 VPN 防火墙前方的 NAT 机制
- 掉线侦测功能(DPD)：若选择此项目勾选，则连接的 VPN 隧道中会定期的传送 HELLO/ACK 讯息数据包来侦测是否 VPN 隧道的两端仍有联机存在。当有一端断线则 VPN 防火墙会自动断线，然后再建立新联机。使用者可以选择每一次 DPD 讯息数据包传递的时间，默认值为 10 秒

### 10.1.3. PPTP 设置

提供支持 Window XP/2000 的 PPTP 对我们 VPN 防火墙做点对点隧道协议，让远程单机用户使用此种协议建立 VPN 联机。

| VPN虚拟专用网 |
|---|
| VPN 状态 |
| 网关对网关设定 |
| 客户端对网关设定 |
| PPTP配置 |
| PPTP状态 |
| VPN数据包穿透 |

☑ 激活 PPTP服务器

**PPTP 用户使用IP范围**

| | |
|---|---|
| 起始IP地址： 10 . 10 . | 10 . 150 |
| 结束IP地址： 10 . 10 . | 10 . 199 |

**远程用户配置**

用户名：

密码：

再次输入密码：

增加到对应列表

删除选中的项目

激活 PPTP 服务： 当使用者勾选后即可以激活点对点隧道协议 PPTP 服务器

PPTP 用户使用 IP 范围： 请输入近端 PPTP IP 地址的范围，其目的是要给远程的使用者一个可进入近端网络的入口 IP。输入起始范围 Range Start:请在最后一栏

输入数值。输入结束范围 Range End：请在最后一栏数入数值

用户名：　　请输入远程使用者的名称

密码的输入与确认：　　输入使用者帐号密码及请再次确认输入远程使用者新的帐号密码

增加到对应列表：　　新增输入的帐号与密码

删除选中的项目：　　删除用户

所有的 PPTP 通道状态：显示所有连接成功的用户，包括使用者名称、远程 IP 地址和 PPTP 发放的地址




**PPTP 用户连接列表**

| 用户名 | 远程用户的IP地址 | 本地对映的IP地址 |
|---|---|---|
| test001 | 60.248.180.226 | 192.168.1.151 |

刷新

10.1.4. 数据包穿透 VPN 防火墙功能（VPN Pass Through）







| IPSec 数据包穿透： | ⦿ 激活 ○ 关闭 |
|---|---|
| | ⦿ 固定来源端口 ○ 变更来源端口 |
| PPTP 数据包穿透： | ⦿ 激活 ○ 关闭 |
| L2TP 数据包穿透： | ⦿ 激活 ○ 关闭 |

确定 取消

| | |
|---|---|
| IPSec 数据包穿透 VPN 防火墙功能: | 若是选择激活 的话，则允许 PC 端使用 VPN- IPSec 数据包穿透 VPN 防火墙以便与外部 VPN 设备联机 |
| 固定来源端口<br>或<br>变更来源端口： | 在 VPN 联机是以 Cisco VPN Server 与 Cisco VPN Client 的状况下才有需要用的此选项，因为 VPN Server 不接受先后两笔用同一个 IP 地址以及同一个 Source Port 的第二笔联机，所以第二笔联机需要变更 Source Port，此时就需要选择 Change Source Port 将原来以 UDP 500 的 Source Port 改成另外随机的 Source Port 联机，选择 Fixed 代表不变更 Source Port 仍以 UDP 500 联机 |
| PPTP 数据包穿透 VPN 防火墙功能: | 若是选择激活 的话，则允许 PC 端使用 VPN-PPTP 数据包穿透 VPN 防火墙以便与外部 VPN 设备联机。 |
| L2TP 数据包穿透 VPN 防火墙功能: | 若是选择激活 的话，则允许 PC 端使用 VPN-L2TP 数据包穿透 VPN 防火墙以便与外部 VPN 设备联机。 |

设置修改完成请按下“确定”按钮储存网络设置变更或是按下“取消”按钮不做任何设置变更。

## 10.2. QnoKey

介绍 Qno VPN 防火墙进行用户端数据的初始设置以及配合 QnoKey 管理软件如何设置 QnoKey 用户端，成功烧制 QnoKey。

### 10.2.1. QnoKey 总表页面

登录 VPN 防火墙后，点开 QnoKey 菜单选项，将出现目前 QnoKey 状态信息摘要总表页面，如下图所示：





QnoKey
设置与连接状态

| IPSec + QnoKey隧道数： | 0 条已经设定使用 | 200 条可用隧道 | 高级设定 |
|---|---|---|---|
| QnoKey隧道数： | 0 条已经设定使用 | 50 条可用隧道 | |

QnoKey 用户连接列表

跳到 1 / 1 页　　每页显示 5 笔

| No. | 激活 | 帐户 | 本地 IP地址 (域名 ) | 有效时间 | 剩余时间 | 使用人数上限 | 已发放人数 | 在线人数 | | | 删除 |
|---|---|---|---|---|---|---|---|---|---|---|---|

新增 QnoKey群組　删除所有群組

刷新

| | |
|---|---|
| IPSec+QnoKey 隧道数 | 显示 IPsec+QnoKey 总共隧道数。表示有几条已经设置使用，以及目前总隧道数。 |
| QnoKey 隧道数 | 表示有几条已经设置使用，以及目前总隧道数。使用者可以透过高级设置自行调整 IPSec 与 QnoKey 隧道数。 |
| 激活： | 表示 QnoKey 用户名称是否启用状态 |
| 帐户： | 显示 QnoKey 的用户名称群组 |
| 本机 IP 地址(网域名称) | 服务器 IP 地址或所使用的域名 |
| 有效时间： | 所设置的 QnoKey 的使用期限,永久使用则会在此显示永久 |
| 剩余时间： | 如设置 QnoKey 使用天数，则在此显示设置后还可使用的有效剩余时间 |
| 使用人数上限： | 表示此用户名称群组设置可以允许烧制的 QnoKey 数 |
| 已发放人数 | 显示已经烧制的 QnoKey 数 |
| 在线人数： | 显示当前在线联机使用 QnoKey 数 |
| 显示用户： | 显示已经设置的 QnoKey 所有使用者列表 |
| 删除 | 删除一条使用名称群组设置规则 |

| | |
|---|---|
| 跳到 1 页 | 选择跳至信息摘要第几页 |
| 5 每页显示的字段 | 总表页面每页显示几条群组信息 |
| 新增 Qnokey 群组： | 增加新的群组设置 |
| 删除所有群组： | 清除所有群组设置。 |

10.2.2 群组设置页面

按下“新增 Qnokey 群组”按钮后，将进入“群组参数设置”页面，如下图所示。

**群组参数设定**

☑ 激活此群组

| | |
|---|---|
| 群组帐户： | |
| 接口位置： | ☐ 广域网1 0.0.0.0 (IP地址/域名) |
| | ☐ 广域网2 220.130.188.40 (IP地址/域名) |
| | ☐ 广域网3 0.0.0.0 (IP地址/域名) |
| | ☐ 广域网4 0.0.0.0 (IP地址/域名) |
| 有效时间： | ⦿ 永久 ○ 日 |
| 使用人数上限： | (最多: 100 人) |
| Key 遗失保护措施： | 禁止连接 |

返回 确定 取消

这个页面主要用来设置 QnoKey 群组。在这里，通过广域网埠口、有效时间、使用者上限人数、遗失保护措施等，对 QnoKey 的群组参数进行设置，以便对 QnoKey 使用者分类管理，提高其安全性。

| | |
|---|---|
| 激活此群组： | 勾选此选项，激活这条设置群组。 |
| 群组帐户名称： | 在此填写想要建立的 QnoKey 群组名称。 |
| 接口位置： | 勾选设置广域网埠口，并填写各广域网埠口相对应的正确的 IP 地址或域名(经 DDNS 解析)。如有广域网埠口为空则不需要填 |





写 IP，以免造成 VPN 连接不成功。此操作设置允许用户从哪一广域网埠连进来，便于管理工作。

当选定广域网 1，则此 QnoKey 群组用户只能通过广域网埠 1 连进来。若同时勾选广域网 1，广域网 2，则允许此 QnoKey 群组用户通过广域网 1 或广域网 2 连接 VPN，当广域网 1 断线则会自动转向广域网 2，作为 VPN 连接备援。

请注意：

- 若勾选的广域网埠口，在网络连接类型为静态 IP 的话，系统会自动显示出此广域网 IP，管理端不需自己再输入。
- 若勾选的广域网埠口，在网络连接类型为 DHCP/PPPoE 等其它类型的话,管理端则需要输入正确的 IP 地址或域名(经 DDNS 解析)。

有效时间：

在这里设置此 QnoKey 群组的有效使用时间。

当用户端 QnoKey 使用比较固定，可点选"forever"选项，设置用户端有效使用时间为永久使用。

如果用户端使用情况比较复杂，或提供给出差移动用户使用，为确保 VPN 数据安全，可设置 QnoKey 使用有效期限为几天，这里允许设置"1~99"天，可根据实际需要填写想设置的天数。

使用人数上限：

这里填写此群组设置规则所允许烧制 QnoKey 的最大数

Key 遗失保护措施：

在下拉菜单中选择 QnoKey 遗失后所进行的操作选项。

如果 QnoKey 不小心意外遗失，可采取三种操作 "不做任何防护"、"清除 Key 内容"和"封锁连机"。

对 QnoKey 进行此项设置，可以进一步提高 VPN 的安全性。选择"不做任何防护"操作选项，则当这把 Key 遗失后，不做任何操作。

选择"清除 Key 内容"操作选项，会在这把 QnoKey 遗失后再



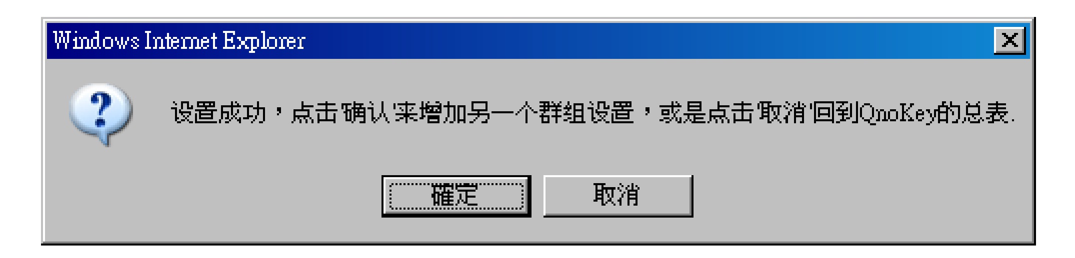


建立 VPN 联机时，将这把 QnoKey 里的数据清除。

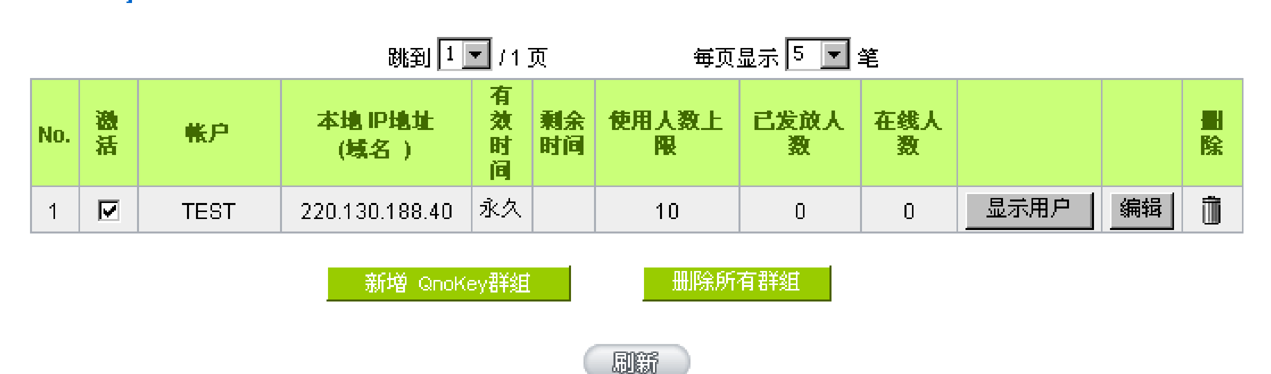
选择"封锁连机"操作选项，则会在这把 Key 遗失后，不能再连上 VPN，将其锁定。

按下“确定”按钮应用此群组设置规则，按“取消”取消刚才的设置操作。按“返回上一页”返回上一页。

当按下“确定”按钮，会弹出一个对话框，询问您是否继续增加设置群组，点击“确定”继续增加另一个群组设置规则，点击“取消”返回到 QnoKey 总表。如下图所示。




这时在 QnoKey 群组信息总表页面就会显示出刚设置好的群组。如下图所示。




| No. | 激活 | 帐户 | 本地 IP地址 (域名 ) | 有效时间 | 剩余时间 | 使用人数上限 | 已发放人数 | 在线人数 | | | 删除 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ☑ | TEST | 220.130.188.40 | 永久 | | 10 | 0 | 0 | 显示用户 | 编辑 | |

当新增规则后，每一条规则后面都会出现“显示用户”和“编辑”按钮。点击“显示使用者”按钮，则会显示应用这条群组规则的用户列表。点击“编辑”按钮编辑修改设置。点击垃圾桶图标，删除这条设置。

### 10.2.3 群组用户列表页面

点击“显示用户”按钮后，将显示应用这条群组规则的群组用户列表页面。

**群组用户列表**

**群组帐户：** test

| No. | 激活 | QnoKey序列号 | 用户名 | 状态 | Key遗失保护措施 | 硬件绑定 | MAC地址 | 删除 |
|---|---|---|---|---|---|---|---|---|

返回 确定 取消

| | |
|---|---|
| 群组帐户名称： | 显示此用户所在群组的名称。 |
| 激活： | 勾选此选项，激活此 QnoKey 用户。 |
| QnoKey 序列号： | 显示此 QnoKey 的序列号。 |
| 用户名： | 显示此 QnoKey 的用户名。 |
| 状态： | 显示此 QnoKey 的联机状态，“联机”表示用户已经联机在线；“不在线”表示没有在线联机使用。 |
| Key 遗失保护措施： | 勾选表示此 QnoKey 遗失，则应用所设置 QnoKey 遗失后的操作。 |
| 硬件绑定： | 若启硬件绑定，QnoKey 只能在所设置绑定 MAC 地址的计算机上使用执行，不是该 MAC 地址数据的计算器，无法使用 QnoKey |
| MAC 地址： | 若有启用硬件绑定功能，会显示 QnoKey 所绑定的计算器 MAC 地址信息，不是该 MAC 地址数据的计算器，无法使用 QnoKey |
| 删除： | 删除该单一用户的 QnoKey 连机数据 |

## 10.3. QVM VPN 功能设置

搭配 QVM 系列 VPN 防火墙提供了三大便利性功能：

1. SmartLink IPSec VPN：简单建立 VPN，取代传统 VPN 建立的复杂缺点，只需要服务器 IP、用户名及密码就可以完成。
2. 中央控管功能：让所有外点或分公司的 VPN 联机状态清楚且可直接在 VPN 防火墙中控画面，远程进入外点客户端做设置。
3. VPN 断线备份机制：让 ISP 断线困扰造成外点或分公司资料无法对总公司传送问题顺利解决。





### 10.3.1. QVM 中心服务器端设置

选择 QVM 功能为服务器模式：




**QVM 配置模式**

QVM 服务器

**QVM 服务器设置**

帐户：

密码：

再次输入密码：

IP地址：10 . 10 . 10 . 0

子网掩码：255 . 255 . 255 . 0

VPN HUB 功能：

激活：

增加到对应列表

删除选中的项目

确定 取消

帐户名称： 需要跟远程客户端名称一致，请输入远程客户端使用者的名称，中英文皆可





密码:/再次输入密码： 需要跟远程客户端密码一致，请输入使用者密码及再次确认使用者密码

IP 地址/子网掩码: 此为 VPN 防火墙内部哪一个网段 IP 地址以及子网掩码，需要跟远程客户端做 QVM 联机

VPN Hub 功能： 分点与总部连通后，可以让分点之间实现互联互通，不用再去各分点的设备之间建立通道，方便管理，更能节省资源。不同运营商电信网通线路可透过总部中央点进行转换，让联机速度不延迟，解决跨网 VPN 联机很卡的问题。同时还能结合侠诺专长的带宽管理功能，让总部的网管人员可以控制不同分支持点间的互相联机，达到更严密控管的功能。

激活: 启用此帐号

增加到对应列表: 新增输入的帐号与密码

删除选中的项目: 删除所选择的使用者

设置修改完成请按下“确定”按钮储存网络设置变更或是按下“取消”按钮不做任何设置变更。

## 10.3.2. QVM 中央控管（QVM 连接状态查询）

用户可以通过点击远程用户的名称登录远程客户端 VPN 防火墙对远程网络进行相关设置。




**QVM 用户连接列表**

| No. | 帐户 | 状态 | 接口位置 | 启动时间 | 结束时间 | 持续时间 | 连接控制 | 配置 |
|---|---|---|---|---|---|---|---|---|

刷新

帐户: 此为用户的外点客户端所显示的用户名称。绿色表示已经连通，蓝色表示等待联机，红色表示此条 QVM 关毕

状态: 此为显示此条 QVM VPN 的联机状态。红色线表示断线，绿色线表示已经连通

接口位置: 此为远程此条 QVM 现在经由 VPN 防火墙的哪一条 WAN 口进来做 QVM 联机

启动时间: 表示此条 QVM 的起用时间

结束时间: 表示此条 QVM 最后的结束时间

持续时间: 表示此条 QVM 启用至结束的总时间

连接控制: 表示现在此条 QVM 所处于的状态：等待联机-Waiting，断开-Disconnect 将此条 QVM 断线并关毕-Disable 此功能，激活开启此条 QVM 至等待联机状态

设置： 若您按下 Edit 按钮， 将会联机到此设置的项目当中，您可以修改其中的设置

### 10.3.3. QVM 用户端设置

选择 QVM 功能为用户端模式:

选择进行 VPN 连接的 VPN 防火墙为 QVM 用户端。

## QVM 配置模式

QVM 用户端

## QVM 用户端设置

帐户： 1

密码： ●●●●●●●●●

再次输入密码： ●●●●●●●●●

QVM VPN： 59.124.169.235 连接

(IP地址或动态域名)

状态： 掉线

☑ 保持连接，如断线 5 分钟后自动重新连接

☑ QVM 备援隧道

QVM 备援隧道1： (IP地址或动态域名)

QVM 备援隧道2： (IP地址或动态域名)

QVM 备援隧道3： (IP地址或动态域名)

## 高级设置

更改QVM用户端服务端口： 443

| | |
|---|---|
| QVM 用户帐户名称： | 输入已在 QVM 服务端中建立的对应用户名称 |
| 密码： | 输入已在 QVM 服务端中建立的对应密码 |
| 再次输入确认密码： | 再输入一次确认密码 |
| QVM VPN（中心端 IP 地址或动态域名）： | 输入 QVM VPN 服务端 IP 地址或是网域名 |
| 状态： | 在此字段可以看到 QVM 功能联机状态 |
| 保持连接，如断线( )分钟后自动重新连接 | 此功能为 QVM 联机断开后，重新检测连接的间隔时间。时间范围为 1~60 分钟 |
| QVM 备援隧道： | 若是勾选此选项，QVM 备援功能将被开启。您可以输入最多三 |





个备援连接 IP 或是网域名，一旦断线可从中心服务端 VPN 防火墙的另一个 WAN 端口自动建立 VPN 联机，确保 VPN 服务永不断线，保证数据传输的安全

设置修改完成请按下“确定”按钮储存网络设置变更或是按下“取消”按钮不做任何设置变更。





十一、虚拟绕径设置

虚拟绕径功能让单线分点轻松晋级享有双线传输，只有单线的企业分点通过设置连线至具有双线的中心端，通过中心点转发到另一条线路出去，加速区域间电信网通连线，解决了连线瓶颈问题。

跨网带宽受限
联机速度很卡
网通
电信
网通单一线路
WAN1
连接电信WEB、
电信游战都很卡
A：单线网吧
网通
电信
WAN2
WAN4
WAN1
WAN3
电信、网通多线路
连网速度超快、
玩游战顺畅不卡
B：多线网吧

如上图：A 网吧只有网通单线传输，由于跨网带宽受限，通过网通去访问电信的 WEB，电信游戏等联机速度很慢，运行起来很卡。而 B 网吧拥有电信网通多线路传输，这样无论访问网通还是电信，连网速度都很快，玩起游戏等也顺畅不卡，满足了用户的需求。

虚拟路由:
A网吧由网通线路
通过配置联机至B网吧
转发到电信线路出去。
单线A网吧解决跨网带宽受限问题
轻松晋级享有双线传输效益

网通
WAN1
网通单一线路
连接电信WEB、
电信游战不再卡了
A: 单线网吧

网通
电信
WAN1
WAN2
WAN3
WAN4
借线
电信、网通多线路
连网速度超快、
玩游战顺畅不卡
B: 多线网吧

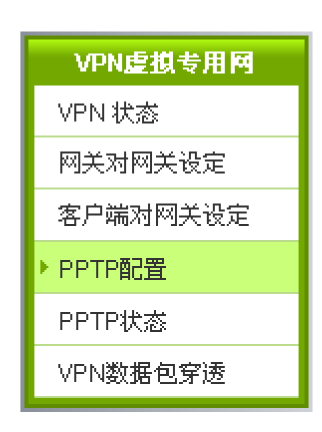
如上图：在这样情况下，A 网吧通过设置路由，由网通线路联机到 B 网吧的 VPN 防火墙，通过 VPN 防火墙转发到电信线路上，这样就好像 A 网吧也配备了电信网通双线路，当 A 网吧用户需要访问电信时，速度不再卡，游戏也变得顺畅，解决了跨网带宽受限的问题，让只有网通单线的 A 网吧轻松晋级享有网通电信双线传输的效益。






11.1 虚拟绕径服务端（PPTP 服务器）

本节主要介绍虚拟遶径服务端如何设置。虚拟遶径是利用 PPTP 建立在 PPP（点对点协议）的基础，它提高了 PPP 的安全级别，让 PPP 可以对 PPTP 服务器与 PPTP 客户端之间的数据进行加密传输，并使 PPTP 服务器可以对远程用户的身份进行验证。进入虚拟绕径项目，勾选"激活 PPTP 服务器"选项，开启 PPTP 服务器。



☑ 激活 PPTP服务器

**PPTP 用户使用IP范围**

| 起始IP地址： | 10.10. 10 . 150 |
|---|---|
| 结束IP地址： | 10.10. 10 . 199 |

**远程用户配置**

用户名：

密码：

再次输入密码：

增加到对应列表

删除选中的项目

PPTP 用户使用范围：是当您联机到 PPTP 服务器后，由服务器分发给客户端的 IP 地址范围。您可以根据需要设置开始 IP 和终止 IP。

新增使用者：在此添加客户端欲进行连接的名称和密码，更新使用者列表。

| 用户名称： | 在此添加客户端欲进行连接的使用者名称 |
|---|---|
| 密码： | 在此输入客户端欲进行连接的密码 |
| 再次输入密码 | 再次输入密码进行身份验证 |
| 更新使用者 | 点此按钮添加或更新到对应列表 |
| 删除使用者 | 点此按钮删除列表中选中的使用者 |
| 新增 | 点此按钮新增使用者到对应列表 |

所有的 PPTP 通道状态：显示所有连接成功的用户，包括使用者名称、远程 IP 地址和 PPTP 发放的地址。





## PPTP 用户连接列表

| 用户名 | 远程用户的IP地址 | 本地对映的IP地址 |
|---|---|---|

刷新

## 11.2 虚拟绕径客户端




### 虚拟绕径

☑ **激活**

| | | |
|---|---|---|
| **绑定接口位置：** | Wan1 | |
| **绑定服务网段：** | 网通网段 | 重新导入网段 |
| **绑定服务端口：** | All | 重新导入端口 |
| | 当连接中断后，每隔 30 分钟重拨 | |
| **远程服务器IP地址：** | 0 . 0 . 0 . 0 | |
| **用户名：** | | |
| **密码：** | | |
| **状态：** | | |

确定　取消

| | |
|---|---|
| 激活虚拟遶径功能 | 勾选此选项,开启虚拟策略路由功能 |
| 绑定接口位置 | 选择虚拟遶径绑定的广网域 WAN 口：WAN1～WAN4 |
| 绑定服务网段 | 在此选择设置预走虚拟绕径的网域，可选择网通或是自定义。这里您可以根据实际需要自己设置绑定的网域。 |
| 重新导入网段 | 点此按钮修改虚拟策略路由 IP 段，点击浏览汇入自定义 IP 文件。（自定义 IP 文件的编写见此表后文件编写 1） |
| 绑定服务端口 | 在此选择设置预走虚拟绕径的端口，可选择所有端口、游戏端口或是自定义。这里您可以根据实际需要自己设置绑定的服务端口。 |
| 重新导入端口 | 点此按钮修改虚拟策略路由服务端口，点击浏览汇入自定义端口文件。（自定义端口文件的编写见此表后文件编写 2） |
| 当连接中断后,每隔 30 : | 此处填写当虚拟绕径中断连接时,重新尝试再次连接的时间间隔,默认为 30 分钟。您可以根据需要填入自定的时间间隔。 |





| 分钟重拨 | |
|---|---|
| 远程服务器 IP 地址 | 在此填写虚拟遶径服务器的外部 IP 地址。 |
| 用户名称 | 在此输入虚拟遶径使用者的名称。 |
| 密码 | 在此输入虚拟遶径服务器的密码。 |
| 状态 | 显示虚拟绕径连接状态：联机或掉线 |

文件编写 1——自定义 IP 文件

自定义 IP 文件的建立可以用纯文本编辑软件来撰写，例如使用 Windows 系统自带的文本编辑程序"记事本"来建立。将您要指定的目的 IP 地址按照下图的格式写入，例如您要指定的目的 IP 地址范围是从 140.115.1.1 到 140.115.1.255，则在"记事本"中输入 140.115.1.1～140.115.1.255。下一个目的 IP 地址范围则要换行输入。请注意！若是只有一个目的 IP 地址，也需要以同样的格式来书写。例如指定的目的 IP 地址是 210.66.161.54，则必须写成 210.66.161.54～210.66.161.54 格式。存储文件后(扩展名应该是.txt)即可汇入修改虚拟策略路由 IP 段。




文件编写 2——自定义端口文件

自定义 IP 文件的建立可以用纯文本编辑软件来撰写，例如使用 Windows 系统自带的文本编辑程序"记事本"来建立。将您要指定的端口按照下图的格式写入，例如您要指定 TCP/3724~3724 端口，则在"记事本"中输入 TCP/3724~3724。下一个指定端口则要换行输入。存储文件后(扩展名应该是.txt)即可汇入修改虚拟策略路由服务端口。






selfport.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
TCP/3724~3724
UDP/15850~15851
TCP/15779~15779
TCP/9801~9801
TCP/38888~38888
TCP/13000~13001
TCP/5816~5816
TCP/16188~16188
TCP/6299~6299
TCP/7600~7900
TCP/9010~9012
TCP/11002~11008
TCP/6020~6020





## 十二、其它进阶高级功能设置

本章介绍 VPN 防火墙进阶功能的设置，如果内网需要设置服务器提供 Web/FTP 服务等，可以通过虚拟服务器的连接设置设置完成，同时应部分用户需要提供静态路由以及动态路由协议的设置，一对一 NAT 功能的设置解决实体 IP 与虚拟 IP 对应，以及设置动态域名解析服务满足用户获得 ISP 的动态公网 IP 情况下需要建设 Web/FTP 服务器等要求。

### 12.1 DMZ/虚拟服务器

**DMZ Host**

内部DMZ服务器IP地址 (DMZ Host)： 10 . 10 . 0 . 0

**虚拟服务器**

服务端口： 所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

内部IP地址： 10 . 10 . 10 .

激活：

增加到对应列表

删除选中的项目

#### 12.1.1 DMZ 设置

当您将 VPN 防火墙内部的某台 PC 的虚拟 IP 填入到此 DMZ 选项时，VPN 防火墙 WAN1 及 WAN2 的合法 IP 地址会直接对应给此台 PC 使用，也就是说从 WAN 端进来的数据包，若是不属于内部的任何一台 PC，都会传送到这台 PC 上。

在使用"DMZ 主机"功能后，若您要取消此功能必须于在设置虚拟 IP 地址地方填入"0" 的参数，才会停止此功能使用。






点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 点击"取消" 即会清除刚才所变动的修改设置内容参数，此操作必须在确认存储动作之前才会有效。

12.1.2 虚拟服务器设置

若是您在内网需架设服务器（意指对外部的服务主机 WEB、FTP、Mail 等），这个功能可将虚拟服务器主机视为一虚拟的位置，利用 VPN 防火墙的外部合法 IP 地址，经过服务端口的转换，(如 WWW 为 80 端口)，直接存取到内部虚拟 IP 的服务器的服务。例如在设置窗口中，选项填入服务器位置，如 192.168.1.2 且端口是 80 的话，当外部网络要进来存取这个网页时只要键入：

http：//220.130.188.45 (假设此为 VPN 防火墙的外部合法 IP 地址)

此时，就会通过 VPN 防火墙的公网 IP 地址去转换到 192.168.1.2 的虚拟主机上的 80 端口读取网页了。

其它种类的服务器设置，都如以上设置；只要将所用服务器的服务端口以及虚拟主机的 IP 地址填入即可！

**虚拟服务器**

服务端口：所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

内部IP地址：10 . 10 . 10 .

激活：

增加到对应列表

删除选中的项目

服务端口： 在此选择欲开启的虚拟服务器的服务端口号码默认列表，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码默认列表！

内部 IP 地址： 在此填上虚拟服务器所要相对应的内部虚拟 IP 地址，如 192.168.1.100。

激活： 开启此服务功能。





服务端口新增或删除表：　若您所需要的服务端口没有在列表里面，可以利用此功能新增或删除管理服务端口号列表。

增加到对应列表：　增加到开启服务项目内容。

新增或删除管理服务端口

若您欲开启的服务端口项目没有在表列中，您可以点击"服务端新增或删除表"新增或删除管理服务端口号列表，如下图所示：

服务端口新增或删除表 - Windows Internet Explorer

http://10.10.10.1/service0.htm

服务名称：

通讯协议： TCP

端口范围： 到

增加到对应列表

所有端口 [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
SMTP [TCP/25~25]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]
TELNETSSL [TCP/992~992]
DHCP [UDP/67~67]
L2TP [UDP/1701~1701]

删除选中的项目

確定　取消　关閉

完成　網際網路　100%






服务端口名称：　在此自定欲开启的服务端口号名称加入列表中，如 BT 等。

通讯协议：　在此选择欲开启的服务端口号的数据包格式为 TCP 或 UDP。

服务端口的位置范围：　将您所需新增加的服务端口范围填入。

增加到对应列表：　增加到开启服务项目内容列表，最多可新增 100 组。

删除选中的项目：　删除所选择的开启服务项目之一笔内容。

确定：　点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。

取消：　点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

离开：　离开此功能设置窗口。

12.1.3 特殊应用软件设置：

有一些特殊应用软件其进出互联网的服务端口号为非对称的，此时您必须使用此功能选项将一些特殊应用程序使用的服务端口号填入相关设置中，如以下窗口所示：

**特殊应用软件**

特殊应用软件名称：

实际对外的端口范围：　到

内部映射的端口范围：　到

增加到对应列表

删除选中的项目

显示开启表　确定　取消

特殊应用软件名称：　您可以自定此特殊应用软件名称，方便管理使用！

实际对外的端口范围：　输入由 VPN 防火墙出互联网的使用端口(Port Number)编号(如 9000~10000)。





| | |
|---|---|
| 内部映射的端口范围： | 输入由互联网进入的使用端口(Port Number)编号。（如2004~2005）。 |
| 增加到对应列表： | 增加到开启服务项目内容列表。 |
| 删除所选中的项目： | 删除所选择的开启服务项目之一笔内容。 |
| 显示开启表： | 点击此按钮即会显示列表上的所有设置项目内容参数。可以以"虚拟主机服务器"和"特殊应用软件"分别来查看列表。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |

12.2 UPnP 通讯协议

UPnP (Universal Plug and Play) 是微软所制定的一项通讯协议标准，若是您使用的计算机有支持 UpnP 机制的话(如 Windows XP)而且您的计算机 UpnP 功能有开启，您可以将 VPN 防火墙的 UPnP 功能启动，可以从您的计算机上开启或关闭 UPnP Forwarding 的选项。

UPnP 功能包含有 UPnP Forwarding 的功能，如您要在内网设置虚拟服务器，您可以在前章节介绍的 Forwarding 功能设置，或是在此 UPnP Forwarding 中设置。不过请不要重复输入造成冲突。

是否激活UPnP自动映射功能： ○ 是 ◉ 否

UPnP手动映射

服务端口： DNS [UDP/53->53]

服务端口新增或删除表

主机名称 或 IP地址：

激活： ☐

增加到对应列表

删除选中的项目

显示开目表 確定 取消

| | |
|---|---|
| 服务端口： | 在此选择欲开启的 UPnP 的服务号码默认列表，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码默认列表！ |
| 主机名称或 IP 地址： | 在此填上 UPnP 相对应的内部虚拟 IP 地址或名称，如 192.168.1.100。 |
| 激活： | 开启此服务功能。 |
| 服务端口增加或删除表： | 新增或删除管理服务端口号列表。 |
| 增加到对应列表： | 增加到开启服务项目内容。 |

| | |
|---|---|
| 删除所选中的项目： | 删除所选择的开启服务项目之一笔内容。 |
| 显示开启表： | 显示目前所开启设置的 UpnP Forwarding 列表。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |

## 12.3 路由通讯协议

此节介绍动态路由协议以及静态路由的设置。

**动态路由**

| 工作模式： | ⦿ NAT模式 ○ 路由模式 |
|---|---|
| RIP路由协议功能： | ○ 激活 ⦿ 关闭 |
| RIP路由协议版本(接收端)： | Both RIP v1 and v2 |
| RIP路由协议版本(传送端)： | RIPv2 - Broadcast |

**静态路由**

目的IP地址：

子网掩码：

网关：

路由节点数：

接口位置：局域网

增加到对应列表

删除选中的项目

### 12.3.1 动态路由设置

RIP 是路由通讯协议 Routing Information Protocol 的简称，有 RIP I / RIP II 两个版本。对于一般使用的网络中，大多只有一个路由器(或是网关器)，所以大部份的情况是不需要使用这个功能。RIP 的使用时机是您的网络中有数个 VPN 防火墙，此台 VPN 防火墙是其中之一，此时若是不想手动设置每台 VPN 防火墙的绕径表，可以启动此功能，自动将所有路径更新！

RIP 是一个很非常简单的路由协议，采用距离向量的方式以数据包到达目的地之前需要经过的路由的个数来做传送距离的判断，而不以实际联机的速率来做判断。所以所选的路径是经过最少的路由，但是并不一定反

应速度最快的路由及路径。

### 动态路由

| 工作模式： | ⦿ NAT模式 ○ 路由模式 |
|---|---|
| RIP路由协议功能： | ⦿ 激活 ○ 关闭 |
| RIP路由协议版本(接收端)： | Both RIP v1 and v2 |
| RIP路由协议版本(传送端)： | RIPv2 - Broadcast |

| | |
|---|---|
| 选择 VPN 防火墙工作模式： | 选择 VPN 防火墙运作模式为 NAT 模式或是路由模式。 |
| 动态路由通讯协议 RIP 功能： | 选择按钮"激活"开启使用 RIP 动态路由通讯。 |
| RIP 路由协议版本（接收端）: | 可于上下选择按钮选择使用动态路由通讯 None， RIPv1， RIPv2，Both RIPv1 and v2 作为传送动态路由通讯协议格式。 |
| RIP 路由协议版本（传送端） | 可于上下选择按钮选择使用动态路由通讯 None， RIPv1，RIPv2-Broadcast， RIPv2-Multicast， 为接收动态路由通讯协议格式。 |

12.3.2 静态路由设置

静态路由是以手动设置路由表的方式来达成数据包路由。在此 VPN 防火墙的应用可分为两种方式，一是在内网中连结不同网段或 VPN 防火墙，一是在 Multi-WAN 的环境中让 VPN 防火墙知道去那个目地地址时就要走那条 WAN。例如常常会遇到 VPN 防火墙不同的 WAN 申请不同家的 ISP 的线路，为了避免有些服务像是邮件服务器，或游戏服务器是架设在不同一 ISP 环境而且 ISP 之间无法彼此互通，此时去邮件服务器或是去游戏服务器就应该走不同的 WAN，而避免绕远路。这个用意跟协议绑定是有相似的做用。






## 静态路由

目的IP地址：
子网掩码：
网关：
路由节点数：
接口位置：局域网
增加到对应列表
删除选中的项目

显示开目表　确定　取消

| | |
|---|---|
| 目的 IP 地址和子网掩码： | 填入目的地的远程网络 IP 节点与子网络节点地址。 |
| 默认网关： | 从此网络节点到目的远程网络欲绕径的默认网关器地址。 |
| 路由节点数： | 从此网络节点到目的远程网络所经过 VPN 防火墙层数，如是在 VPN 防火墙下的二个 VPN 防火墙之一，此应填为 2，默认为 1。(最大为 15)。 |
| 接口位置： | 此网络节点的连接位置，是位于广域端口 WAN 端亦或是局域端口 LAN 端。 |
| 增加到对应列表： | 增加此路径规则到列表中。 |
| 删除所选中的项目： | 删除在表中所选择的路径表。 |
| 显示开启表： | 显示目前最新的路径表。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |

## 12.4 一对一 NAT 对应

当您的 ISP 线路为固定制(如 ADSL 固定 IP)时，通常 ISP 会给您多个合法 IP 地址。VPN 防火墙提供您可将除了 VPN 防火墙本身 WAN 端口以及光纤盒或 ATU-R(网关) 各使用一个合法 IP 地址后，所剩的合法 IP 地址可以直接对应到 VPN 防火墙内部的计算机使用，也就是这些计算机在内网虽为虚拟 IP，但当做了一对一对应后，这些对应到的计算机去外部访问时都是有自己的合法 IP。

例如，当您公司内部环境需有两台或两台以上的"WEB 服务器"时，由于需要两个或两个以上的合法 IP 地址，所以可以利用此功能达到将外部多个合法 IP 地址直接对应到内部多个虚拟服务服务器 IP 地址使用！

范例： 如您有 5 个合法 IP 地址，分别是 210.11.1.1～6，而 210.11.1.1 已经给 VPN 防火墙的 WAN1 使用，另外还有其它四个合法 IP 可以分别设置到 One to One NAT 当中，如下所述：

210.11.1.2→ 192.168.1.3

210.11.1.3→ 192.168.1.4

210.11.1.4→ 192.168.1.5

210.11.1.5→ 192.168.1.6

---

注意！

VPN 防火墙 WAN IP 地址不能被涵盖在一对一 NAT 的 IP 范围设置中。

---





☑ 激活一对一NAT 功能

内部起始IP地址：10 . 10 . 10 .
外部起始IP地址：. . .
对应范围的IP数量：
增加到对应列表

删除选中的项目

确定 取消

| | |
|---|---|
| 激活一对一 NAT 功能: | 选择是否开启此一对一 NAT 功能 "激活"开启 "禁止"关闭。 |
| 内部起始 IP 地址: | 虚拟 IP 地址起始 IP 地址。 |
| 外部起始 IP 地址: | 外部合法 IP 地址起始 IP。 |
| 对应范围的 IP 数量: | 填入您同时要有多少个外部合法 IP 地址需要对应。 |
| 增加到对应列表: | 加入此设置到一对一 NAT 列表中。 |
| 删除选中的项目: | 删除所选择的一对一 NAT 规则。 |
| 确定: | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消: | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于"确定"存储动作之前才会有效。 |

注意！

一对一的 NAT 模式将会改变防火墙运作的方式，您若设置了此功能，LAN 端所对应有 公网 IP 的服务服务器或计算机将会曝露在互联网上。若要阻绝网络的使用者主动联机到一对一 NAT 的服务服务器或计算机，请到防火墙的存取规则中设置适当的拒绝存取规则条件。





12.5 DDNS-动态域名解析

此 VPN 防火墙的 “DDNS” 功能可以支持 QnoDDNS.org.cn、Dyndns.org、3322.org、Dtdns（支持 DDNS 种类依机种不同而相异）的动态域名解析功能，其目的是为了让使用动态 IP 地址(也就是无法有固定 IP 的环境)来架设虚拟服务器、建立企业 VPN 使用、及远程监控时查询现在的 VPN 防火墙 IP。如 ADSL PPPoE 计时制或是 Cable Modem 的使用者的 WAN IP 地址都会随 ISP 端要求而改变，当此时使用者申请了 DDNS 后，如"qno. QnoDDNS.org.cn"，将其设置在 DDNS 设置中，则在远程只要去 Ping QnoDDNS.org.cn 则可以知道现在 VPN 防火墙的实际 IP。且若是内部有架设网站之类的服务，网络使用者只要在网址打上 qno. QnoDDNS.org.cn 就可以直接进入到您内部架设的 WEB。在设置此功能之前，请向 www.qno.cn/ddns、www.dyndns.org 或是 www.3322.org 提出申请，此服务是完全免费的！

另外，为了解决 DDNS 服务器可能会发生不稳定的情况，现在 VPN 防火墙每个 WAN 都可同时对此三家 DDNS 做动态 IP 升级。

**动态域名服務**

| 接口位置 | 动态域名 | 状态 | 配置 |
|---|---|---|---|
| 广域网1 | Dyndns:---<br>3322:---<br>Dtdns:---<br>Qnoddns:--- | Dyndns 关闭<br>3322 关闭<br>Dtdns 关闭<br>Qnoddns 关闭 | 编辑 |
| 广域网2 | Dyndns:---<br>3322:---<br>Dtdns:---<br>Qnoddns:--- | Dyndns 关闭<br>3322 关闭<br>Dtdns 关闭<br>Qnoddns 关闭 | 编辑 |
| 广域网3 | Dyndns:---<br>3322:---<br>Dtdns:---<br>Qnoddns:--- | Dyndns 关闭<br>3322 关闭<br>Dtdns 关闭<br>Qnoddns 关闭 | 编辑 |
| 广域网4 | Dyndns:---<br>3322:---<br>Dtdns:---<br>Qnoddns:--- | Dyndns 关闭<br>3322 关闭<br>Dtdns 关闭<br>Qnoddns 关闭 | 编辑 |

选择您要设置的广域网端口，比如"广域网 1"，点击"编辑"进入广域网 1 的 DDNS 设置窗口，对要设置的 WAN 口的 DDNS 方式进行勾选。

接口位置: WAN1

☑ DynDNS.org

| | |
|---|---|
| 用户名: | 注册 |
| 密码: | (密码不能含有字符串'password') |
| 动态域名: | . . |
| 广域网 IP地址: | 0.0.0.0 |
| 状态: | DDNS功能关闭或是没有联机 |

☑ 3322.org

| | |
|---|---|
| 用户名: | 注册 |
| 密码: | (密码不能含有字符串'password') |
| 动态域名: | . . |
| 广域网 IP地址: | 0.0.0.0 |
| 状态: | DDNS功能关闭或是没有联机 |

☐ DtDNS.com

☐ QnoDDNS.org.cn

返回 确定 取消

| | |
|---|---|
| 接口位置 | 显示使用者所选取的广域端口 |
| DDNS 动态域名解析服务： | 可以选择 QnoDDNS.org.cn、Dyndns.org 以及 3322.org(可以同时使用)。(支持 DDNS 种类依机种不同而相异) |
| 用户名称： | 向 DDNS 服务提供者所申请的使用者名称。QnoDDN 使用者名称要填入完整的网址，如：abc.qnoddns.org.cn。 |
| 密码： | 向 DDNS 服务提供者所申请的密码。 |
| 动态域名： | 动态网址名称： 向 DDNS 所注册的网址，如 abc.QnoDDNS.org.cn 或者 abc.dyndns.org。 |
| 广域网 IP 地址： | 目前此条 WAN 所取得的 ISP 之动态合法 IP 地址，当 VPN 防火墙得到 ISP 端给的合法 IP 地址后会自动显示于此。 |
| 状态： | 显示目前 VPN 防火墙对 DDNS 的更新状态。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |





注册 QnoDDNS 侠诺动态域名

1． 请先至 Qno 侠诺网站，进行产品注册：http://www.qno.cn

2． 依据产品注册使用的电邮以及产品序列号，登入 QnoDDNS 侠诺动态域名服务系统；请确认电邮可以确实收信，以利注册域名后，可收到系统寄出的启用 QnoDDNS 服务密码。




3． 域名申请规则：

● 域名最少需为 4 个字，最多 63 个字。

● 域名只能由 a-z(英文小写)、0-9(数字)所组成，且第一个字需为英文字母。

● 域名不得有特殊符号(例如："."；"-"；"_"等等) 。

● 2 Wan 系列产品最多申请 2 个 DDNS 设置。

● 4 Wan 系列产品最多申请 4 个 DDNS 设置。

● 8 Wan 系列产品(含以上)最多申请 4 个 DDNS 设置。








:: 用户数据 ::

| 姓名 | |
|---|---|
| Email | |
| 序列号 | |
| 型号 | |
| Wan数量 | |

:: 申请规则 ::

1. 如果您申请Qno侠诺科技动态域名服务，代表您同意侠诺科技动态域名服务条款。
2. "用户名称"最少需要4个字，最多63个字(4-63个字)。
3. "用户名称"只能由a-z(英文小写)、0-9(数字)所组成，且第一个字需为英文字母。
4. "用户名称"不得有特殊符号(例如："."；"-"；"_"等等)。( 范例 )
5. 2 Wan系列产品最多申请2个DDNS设定。
6. 4 Wan系列产品最多申请4个DDNS设定。
7. 8 Wan系列产品(含以上)最多申请4个DDNS设定。

:: Host Name 测试 ::

已输入**0**个字

| 测试 | 用户名称： | | 域名： | qnoddns.org.cn | 发送 重设 |
|---|---|---|---|---|---|

尚可申请 4 组DDNS

已输入**0**个字

| 第1组 | 用户名称： | | 域名： | qnoddns.org.cn | 申请 |
|---|---|---|---|---|---|

已输入**0**个字

| 第2组 | 用户名称： | | 域名： | qnoddns.org.cn | 申请 |
|---|---|---|---|---|---|

已输入**0**个字

| 第3组 | 用户名称： | | 域名： | qnoddns.org.cn | 申请 |
|---|---|---|---|---|---|

已输入**0**个字

| 第4组 | 用户名称： | | 域名： | qnoddns.org.cn | 申请 |
|---|---|---|---|---|---|

## 12.6 广域网接口 MAC 地址设置

有些 ISP 会要求提供一固定 MAC 地址(网卡物理地址)做为 ISP 端分配 IP 给您的认证使用，此大多适用于 Cable Mode 的用户。若有此需求的话，可使用此功能将提供给 ISP 的网卡物理地址(MAC 地址：00-xx-xx-xx-xx-xx)填入此项目中，VPN 防火墙就会以此 MAC 地址作为跟 ISP 请求 IP 时的认证！

### 广域网MAC地址设置

| 接口位置 | MAC地址 | 配置 |
|---|---|---|
| 广域网1 | 00-17-16-01-35-d0 | 编辑 |
| 广域网2 | 00-17-16-01-35-d1 | 编辑 |
| 广域网3 | 00-17-16-01-35-d2 | 编辑 |
| 广域网4 | 00-17-16-01-35-d3 | 编辑 |

选择您要设置的广域网端口，比如"广域网 1"，点击"编辑"进入广域网 1 的端口 MAC 地址设置窗口，使用者可以自行输入提供给 ISP 的网卡物理地址 MAC，点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

目前设备出厂默认的 MAC 位置为 WAN 端的 MAC 地址。

**接口位置:** WAN1

| 使用者自订义广域网接口MAC地址： | ⦿ 00 - 17 - 16 - 01 - 35 - d0<br>(默认值: 00-17-16-01-35-d0) |
|---|---|
| 设定与此PC的MAC地址相同： | ○ bf-ff-f7-95-00-43 |

返回 确定 取消






## 十三、工具程序功能设置

此章节介绍用来管理 VPN 防火墙以及测试网络联机的工具。

考虑安全的因素，建议修改密码。关于登录密码与 VPN 防火墙时间的设置已经在第五章 5.2 节已经介绍，在此就不做重复介绍了。

### 13.1 在线联机测试




VPN 防火墙提供简易的在线测试机制，方便于测试线路质量时使用。此包含 DNS 查询以及 Ping 二种。




域名解析测试

请于此测试窗口输入您想查询的网域主机位置名称，如 www.abc.com 然后点击开始的按钮开始测试。测试结果会显示于此窗口上。





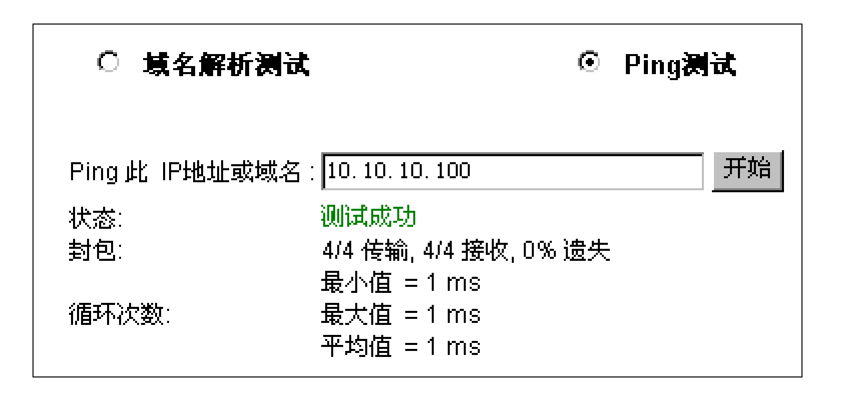
◉ 域名解析测试　　○ Ping测试

测试域名(www.qno.cn)：www.google.com　开始

名称:　www.google.com

地址:　72.14.235.99

Ping-数据包传送/接收测试




此项目为主要提供管理者了解对外联机的实际状况，可以由此功能了解网络上的计算机是否存在！

请于此测试窗口输入您想测试的主机位置 IP，如 168.95.1.1 点击开始的按钮开始测试，测试结果会显示在窗口上。





## 13.2 系统软件更新

此功能可以让 VPN 防火墙在 Web 设置窗口中直接做软件升级。请您于升级前先确认软件版本信息。 点击"浏览"按钮，选择软件存放文件夹，并于选择欲升级的软件后，点击立即系统软件更新做升级。

---

注意！

执行软件升级前，请详细阅读窗口中的注意事项。

正在做软件升级当中时，请勿离开此升级窗口，否则会造成 VPN 防火墙升级失败。

---




**软件更新**




**警告 ：** 1. 当您选择前一个版本的软件时，所有的设定都将回复到出厂预设值
2. 软件升级需要一点时间，此时切勿拔除电源或按下Rest按钮
3. 当您在作软件升级时，请勿关闭此画面或中断此联机

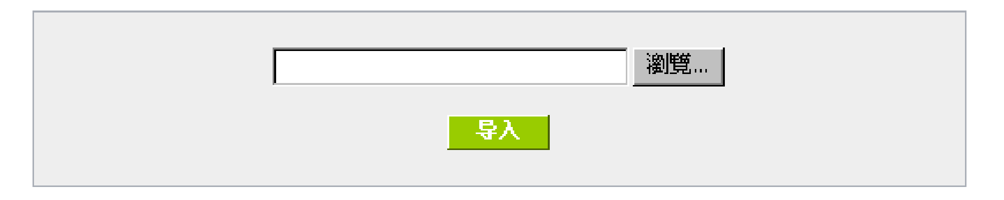





## 13.3 系统设置参数存储




**从指定的配置文件恢复**




**备份目前的配置**

导出

从指定的设置文件恢复：

此功能将之前所存储在计算机的备份设置参数内容回存到 VPN 防火墙中！选择"浏览"至备份参数文件"config.exp"存放数据夹，选择该文件后，点击"导入"按钮做设置文件导入。

备份目前的设置：

此功能为存储网管人员在 VPN 防火墙的设置参数备份到计算机中，通常做 VPN 防火墙版本升级前，请务必将您现在的 VPN 防火墙设置文件用此功能存储在计算机中！点击存储按钮，选择至备份参数文件"config.exp"存放数据夹位置，点击存储即可。






13.4 网络管理设置(SNMP)

SNMP 为 Simple Network Management Protocol 的缩写，指网络管理通讯协议。此为互联网上使用的一个管理工具，通过此 SNMP 通讯协议，可以让已经具备有网络管理的程序(如 SNMP tools-HP Open View)等网管程序做实时管理之通讯使用。VPN 防火墙支持标准 SNMP v1/v2c，可以搭配标准 SNMP 网络管理软件来得知目前 VPN 防火墙上的机器运作情况，以便随时掌握网络信息。

系统工具
- 密码设置
- 自我诊断
- 软件更新
- 配置参数备份/恢复
- SNMP网络管理
- 时间设置
- 系统恢复

SNMP网络管理

☑ 激活

| | |
|---|---|
| 系统名称： | 4_WAN_QVM_Router |
| 联系方式： | |
| 系统地址： | |
| Get Community Name： | public |
| Set Community Name： | private |
| Trap Community Name： | public |
| Send SNMP Trap to： | |

确定 取消

激活： 将 SNMP 功能开启或关闭。系统默认为开启此功能。

系统名称： 设置机器的名称，如 VPN Firewall。

联系方式： 设置机器的管理联系人员名称。





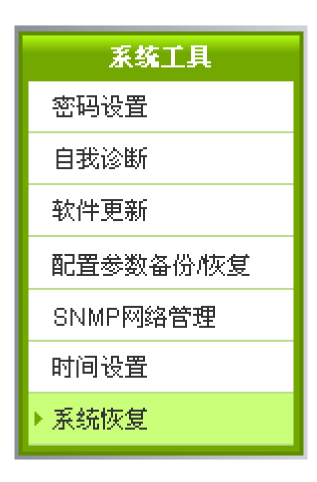
| | |
|---|---|
| 系统地址： | 设置机器的目前所在位置。 |
| Get Community Name： | 设置一组管理者参数可以取得此机器的项目信息，系统默认"Public"。 |
| Set Community Name： | 设置一组管理者参数可以设置此机器的项目信息，系统默认"Private"。 |
| Trap Community Name： | 设置一组管理者参数可以传送 Trap 的信息。 |
| Send SNMP Trap 到： | 设置一组 IP 地址或是域名名称的接收 Trap 讯号主机。 |
| 确定： | 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。 |
| 取消： | 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。 |






## 13.5 系统恢复

您可以于此工具中选择 VPN 防火墙系统重新开机功能，请点击"系统重新启动"的"立即重新激活" 按钮即可重新开机启动。




**重新启动**

立即重新启动

**恢复原出厂设置**

立即恢复原出厂设置

系统重新启动

如图，如果点击系统启动下的"立即重新激活",会弹出提对话框提示是否重新启动 VPN 防火墙，确定 VPN 防火墙就做重新启动操作。

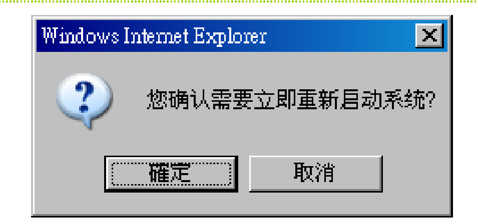





**重新启动**

立即重新启动

**恢复原出厂设置**




恢复原出厂默认值

若是选择重新恢复"立即重新激活"， 会弹出提对话框提示是否恢复出厂值，确定后 VPN 防火墙将做恢复出厂值操作。

**重新启动**

立即重新启动

**恢复原出厂设置**




我们建议在做版本升级前请先将 VPN 防火墙现在的设置值存储在计算机当中，等做完版本升级后，使用此功能将机器做出厂值设置以确保机器升级后的稳定运行，然后再将刚才存在计算机的设置直存回 VPN 防火墙(如何存储 VPN 防火墙的设置数据及升级完成后如何存回 VPN 防火墙，请参考 13.3 系统设置参数存储说明)。



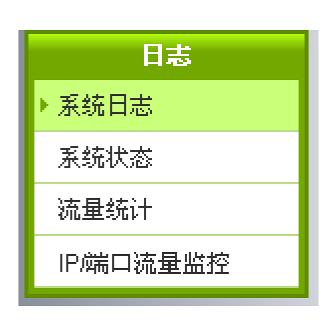



## 十四、日志功能设置

日志功能纪录 VPN 防火墙的运行数据，并以可读的方式呈现再设置窗口上提供给您作为参考。您可以依据需求检视这些信息。

### 14.1 系统日志

VPN 防火墙的日志记录提供三种设置：系统日志， 电子邮件通知，以及选择日志的类别。



### 发送到日志服务器

☑ **激活**

| 主机名称： | 0.0.0.0 | (正确网域名称或IP地址) |
|---|---|---|

### 发送到电子邮箱

☑ **激活**

| **电邮服务器：** | | (正确网域名称或IP地址) |
|---|---|---|
| **电子邮件：** | | |

| **发送数量：** | 50 | 笔 |
|---|---|---|
| **发送间隔时间：** | 10 | 分钟 |

立即发送到电子邮箱

### 系统日志配置

| **告警日志** | | |
|---|---|---|
| ☐ Syn Flooding | ☐ IP Spoofing | ☐ Win Nuke |
| ☐ Ping Of Death | ☑ 登入认证错误 | |

| **一般日志** | | |
|---|---|---|
| ☑ 系统错误信息 | ☐ 被阻挡的管制条例 | ☐ 允许通过的管制条例 |
| ☑ 系统配置变更 | ☑ 认证登入 | |

查看系统日志 | 出去NAT记录 | 进入NAT记录 | 清除日志

系统日志

激活传送到日志服务器： 若是勾选此选项的话，传送系统日志功能将被开启。

系统日志服务器主机名称： VPN 防火墙 提供了外部系统日志服务器收集系统信息功能。系统日志为一项工业标准通讯协议，于网络上动态撷取有关的系统信息。VPN 防火墙 的系统日志 提供了包含动作中的联机来源位置与目的位置，服务编号以及状态。输入您要接收系统日志的服务器名称或是 IP 地址于"系统日志服务器"的空格字段内。






电邮告警功能

| | |
|---|---|
| 激活传送到电子邮箱: | 若是勾选此选项的话，电子邮件告警将会被开启。 |
| 电邮服务器: | 请输入电子邮件服务器的名称或是 IP 地址，如 mail.abc.com。请注意，您必须有权限经由所填入的电子邮件服务器寄送日志电子邮件，否则此日志电子邮件将无法被寄出。 |
| 电邮地址: | 此为设置日志收件人电子邮件信箱，例如 abc@mail.abc.com |
| 传送日志数量: | 自定日志数量，系统默认为 50 条。 当到达此数量时，VPN 防火墙将会自动 Mail 传送日志。 |
| 传送区隔时间: | 自定传送日志间隔时间，系统默认为 10 分钟。 当到达此时间时，VPN 防火墙将会自动 Mail 传送此日志。<br>VPN 防火墙将会自动判别当数量或是间隔时间哪一个参数先到达，就 Mail 传送日志信息给管理者。 |
| 立即传送到电子邮箱: | 使用管理者可以直接按此按钮传送日志。 |

系统日志设置

**系统日志配置**

| 告警日志 | | |
|---|---|---|
| ☐ Syn Flooding | ☐ IP Spoofing | ☐ Win Nuke |
| ☐ Ping Of Death | ☑ 登入认证错误 | |

| 一般日志 | | |
|---|---|---|
| ☑ 系统错误信息 | ☐ 被阻挡的管制条例 | ☐ 允许通过的管制条例 |
| ☑ 系统配置变更 | ☑ 认证登入 | |

查看系统日志 | 出去NAT记录 | 进入NAT记录 | 清除日志

VPN 防火墙 提供了包含以下的告警内容信息，您只要打勾点选即可包含在日志信息中。

| | |
|---|---|
| Syn Flooding： | 即在短时间内传送大量的 syn 数据包，造成系统记录联机的内存溢满。 |
| IP Spoofing： | 通过数据包监听程序来拦截网络上所传送数据，并在读取后藉由程序修改原发送端地址，进入原目的端的系统内，存取资源。 |
| Win Nuke： | 通过侵入或设陷阱的方式将木马程序送入对方服务器中。 |
| Ping of Death： | 通过传送来产生超过 IP 协议所能够允许的最大数据包，造成系统宕机。 |





登录认证错误： 当系统发现有企图登录 VPN 防火墙的入侵者时，就会将信息传到系统日志中。

一般系统日志信息

VPN 防火墙 提供了包含以下的一般性内容信息，您只要打勾点选即可。系统错误信息，被阻挡的管制条例，允许通过的管制条例，认证登录，系统设置变更。

系统错误信息： 提供系统中各种错误给系统日志。例如：不正确的设置或是功能异常状况发生。

被阻挡的管制条例： 当有用户试图进行存取规则中不允许的规则时，此信息会传送到系统日志中。

允许通过的管制条例： 当用户进行存取规则所允许的规则时，此信息会传送到系统日志中。

系统设置变更： 当系统的设置值改变时，此信息回传送到系统日志中。

认证登录： 每一个成功登录系统的 IP 地址都会传送并记录到系统日志中。

以下有四个有关查询日志的按钮，分别叙述如下：

查看系统日志：

此为查看系统日志使用，其信息内容可以从下拉式选单中分类读取，包含全部日志， 系统日志，防火墙日志，VPN 日志。选择"刷新"按钮可以刷新日志显示窗口，"清除"按钮可以清除所有日志记录。如下图所示：

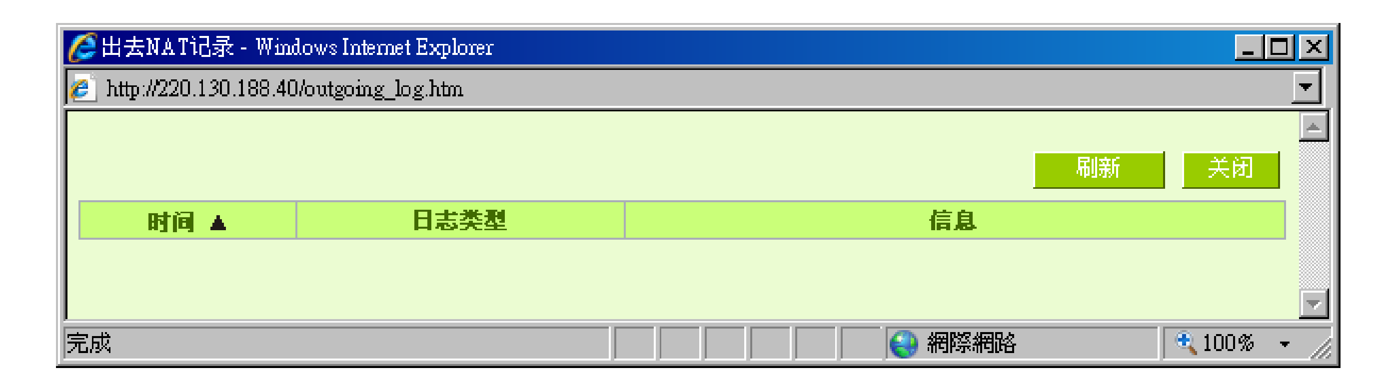



出去 NAT 记录：

查看内部 PC 出互联网的系统数据包日志，此日志包含内部网络地址，目的地地址以及所使用的通讯服务端口号、类型等信息。






进入 NAT 记录：

查看外部进入 VPN 防火墙的系统数据包日志，此日志内含外部来源网络地址， 目的地地址与通讯端口号等信息。




清除日志：

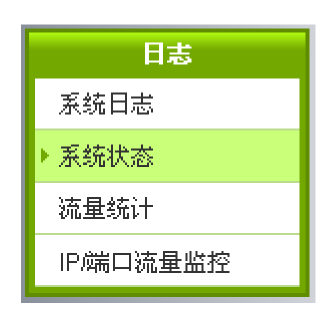
此按钮为清除所有目前 VPN 防火墙的日志相关信息。






## 14.2 系统状态实时监控

VPN 防火墙的系统状态实时监控管理功能可以提供系统目前的运行信息，包含局域或广域端口名称，目前端口联机状态，IP 地址，网络实体位置(MAC 地址)，子网掩码，默认网关，域名解析服务器(DNS)，网络侦测，收到的数据包数量，传送的数据包数量，全部的进出数据包数量统计，收到的数据包 Byte 流量统计，传送的数据包 Byte 流量统计，全部进出的数据包 Byte 流量统计，收到的错误数据包统计以及端口丢弃的数据包统计，会话数，新联机数，上传带宽使用率，下载带宽使用率等信息。



## 系统状态

下一页>>

| 接口位置 | 广域网1 | 广域网2 | 广域网3 | 广域网4 |
|---|---|---|---|---|
| 接口名称 | ixp1 | ixp2 | ixp3 | ixp4 |
| 线路连线状态 | 关闭 | 联机 | 关闭 | 关闭 |
| IP地址 | 0.0.0.0 | 220.130.188.40 | 0.0.0.0 | 0.0.0.0 |
| MAC地址 | 00-17-16-01-35-d0 | 00-17-16-01-35-d1 | 00-17-16-01-35-d2 | 00-17-16-01-35-d3 |
| 子网掩码 | 0.0.0.0 | 255.255.255.240 | 0.0.0.0 | 0.0.0.0 |
| 默认网关 | 0.0.0.0 | 220.130.188.33 | 0.0.0.0 | 0.0.0.0 |
| DNS 服务器 | 0.0.0.0 | 168.95.1.1<br>0.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| 线路侦测机制 | 测试失败 | 测试成功 | 测试失败 | 测试失败 |
| 接收数据包统计 | 0 | 0 | 0 | 0 |
| 传送数据包统计 | 0 | 0 | 0 | 0 |
| 全部数据包统计 | 0 | 0 | 0 | 0 |
| 数据包接收Byte数量 | 0 | 186375184 | 0 | 0 |
| 数据包传送Byte数量 | 0 | 88938703 | 0 | 0 |
| 全部数据包Byte数量 | 0 | 275313887 | 0 | 0 |
| 目前接收流量Bytes/Sec | 0 | 594 | 0 | 0 |
| 目前传送流量Bytes/Sec | 0 | 60 | 0 | 0 |
| 错误数据包统计 | 0 | 0 | 0 | 0 |
| 丢弃数据包统计 | 0 | 0 | 0 | 0 |
| 会话数 | 0 | 14 | 0 | 0 |
| 新会话数/秒 | 0 | 0 | 0 | 0 |
| 上传带宽使用率(%) | 0 | 0 | 0 | 0 |
| 下载带宽使用率(%) | 0 | 0 | 0 | 0 |

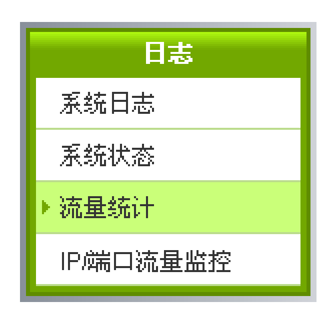
刷新






## 14.3 流量统计

VPN 防火墙提供六种显示流量统计的信息，来提供管理者对于流量有更好的管理与控制。




**流量统计**

☑ **激活**

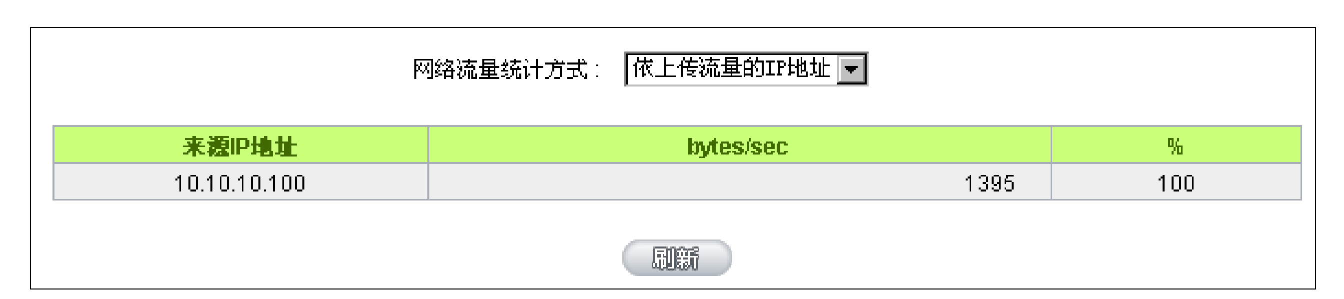
网络流量统计方式： 依下载流量的会话

| 目的IP地址 | 通讯协议 | 目的端口 | 来源IP地址 | 来源端口 | bytes/sec | % |
|---|---|---|---|---|---|---|

刷新

依上传流量的 IP 地址：

在此图表中显示了从外进入内网流量的来源端的 IP 地址， 每秒有多少 byte 与所占的百分比。




| 来源IP地址 | bytes/sec | % |
|---|---|---|
| 10.10.10.100 | 1395 | 100 |

依下载流量的 IP 地址：

在此图表中显示了从内网出去流量的来源端的 IP 地址， 每秒有多少 byte 与所占的百分比。

网络流量统计方式： 依下载流量的IP地址

| 来源IP地址 | bytes/sec | % |
|---|---|---|
| 10.10.10.100 | 8737 | 100 |

刷新

依上传流量的端口：

在此图表中显示了以网络的服务端口来分类进入内网使用流量统计(每秒)byte 与百分比。

网络流量统计方式： 依上传流量的端口

| 通讯协议 | 目的端口 | bytes/sec | % |
|---|---|---|---|
| TCP | 443 | 2862 | 98 |
| UDP | 8000 | 30 | 1 |
| TCP | 1863 | 4 | 0 |

刷新

依下载流量的端口：

在此图表中显示了以网络的服务端口来分类从内网出去的使用流量统计(每秒)byte 与百分比。

网络流量统计方式： 依下载流量的端口

| 通讯协议 | 目的端口 | bytes/sec | % |
|---|---|---|---|
| TCP | 2082 | 160 | 50 |
| TCP | 443 | 70 | 22 |
| TCP | 2083 | 52 | 16 |
| TCP | 1863 | 29 | 9 |

刷新

依上传流量的会话：

在此图表中显示了从广域网络进来的(Dest. IP)地址所联机的局域网络的 IP(Source IP)位置所使用的服务端口(Dest.Port)还有现在使用流量(bytes/sec)与百分比。





网络流量统计方式：依上传流量的会话

| 来源IP地址 | 通讯协议 | 来源端口 | 目的IP地址 | 目的端口 | bytes/sec | % |
|---|---|---|---|---|---|---|
| 10.10.10.100 | TCP | 3802 | 59.124.180.50 | 443 | 30 | 68 |
| 10.10.10.100 | UDP | 4000 | 58.251.60.87 | 8000 | 5 | 12 |
| 10.10.10.100 | TCP | 3803 | 59.124.180.50 | 443 | 4 | 9 |

刷新

依下载流量的会话：

在此图表中显示了从局域网络的 IP(Source IP)地址对外联机的目的地位置(Dest. IP)IP 及所使用的服务端口(Dest.Port)还有现在使用流量(bytes/sec)与百分比。

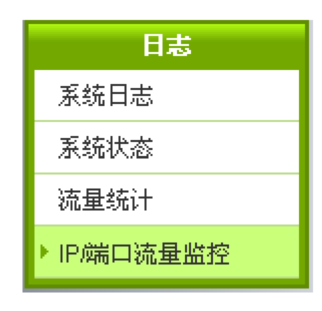
网络流量统计方式：依下载流量的会话

| 目的IP地址 | 通讯协议 | 目的端口 | 来源IP地址 | 来源端口 | bytes/sec | % |
|---|---|---|---|---|---|---|
| 10.10.10.100 | TCP | 3979 | 65.55.15.244 | 80 | 72 | 37 |
| 10.10.10.100 | TCP | 3964 | 122.116.228.7 | 443 | 39 | 20 |
| 10.10.10.100 | TCP | 3980 | 207.46.26.26 | 1863 | 36 | 19 |
| 10.10.10.100 | UDP | 1056 | 168.95.1.1 | 53 | 29 | 15 |
| 10.10.10.100 | TCP | 3328 | 207.46.107.46 | 1863 | 12 | 6 |

刷新

## 14.4 特定 IP 及端口状态

VPN 防火墙提供网管人员可以针对某一 IP 或某一特定端口去查询此 IP 去访问的目的地址，或是有哪些人使用这个服务端口。其目的可以方便找出某些需要认证的网站无法走多 WAN 端口而必须走单一个 WAN 端口，网管人员可以查询出此目的地的 IP 做协议绑定来解决此登录问题。另外，若想查询何人在使用 BT 或 P2P 软件，也可选择 Port 做使用者查询。



**IP/端口流量监控**

☑ 激活

查询方式依 IP地址 IP地址 : 0 . 0 . 0 . 0 查询

| 来源IP地址 | 通讯协议 | 来源端口 | 接口位置 | 目的IP地址 | 目的端口 | 下载带宽 Bytes/Sec | 上传带宽 Bytes/Sec |
|---|---|---|---|---|---|---|---|

刷新

特定 IP 状态：

直接在 IP 地址里填入您想要查询的 IP 地址，就可以显示出此 IP 对外联机的所有目的地及端口号。

查询方式依 IP地址 IP地址 : 10 . 10 . 10 . 100 查询

| 来源IP地址 | 通讯协议 | 来源端口 | 接口位置 | 目的IP地址 | 目的端口 | 下载带宽 Bytes/Sec | 上传带宽 Bytes/Sec |
|---|---|---|---|---|---|---|---|
| 10.10.10.100 | TCP | 3328 | WAN2 | 207.46.107.46 | 1863 | 0 | 0 |
| 10.10.10.100 | TCP | 3351 | WAN2 | 59.124.180.50 | 443 | 4 | 22 |
| 10.10.10.100 | TCP | 3352 | WAN2 | 59.124.180.50 | 443 | 18 | 4 |
| 10.10.10.100 | UDP | 4000 | WAN2 | 58.251.60.87 | 8000 | 70 | 39 |
| 10.10.10.100 | TCP | 3802 | WAN2 | 59.124.180.50 | 443 | 0 | 0 |
| 10.10.10.100 | TCP | 3803 | WAN2 | 59.124.180.50 | 443 | 0 | 0 |
| 10.10.10.100 | UDP | 6001 | WAN2 | 58.251.62.71 | 8000 | 0 | 0 |
| 10.10.10.100 | TCP | 3964 | WAN2 | 122.116.228.7 | 443 | 40 | 25 |
| 10.10.10.100 | TCP | 3977 | WAN2 | 59.124.180.50 | 443 | 0 | 0 |
| 10.10.10.100 | TCP | 3978 | WAN2 | 59.124.180.50 | 443 | 0 | 0 |
| 10.10.10.100 | TCP | 3980 | WAN2 | 207.46.26.26 | 1863 | 4 | 20 |
| 10.10.10.100 | UDP | 1056 | WAN2 | 168.95.1.1 | 53 | 0 | 0 |
| 10.10.10.100 | TCP | 3981 | WAN2 | 208.50.79.27 | 80 | 0 | 0 |
| 10.10.10.100 | UDP | 6007 | WAN2 | 210.22.23.177 | 8000 | 0 | 0 |

刷新

特定端口状态：

直接在端口里填入您想要查询的端口号，就可以显示出此端口现在有哪些 IP 正在使用。

查询方式依 服务端口 服务端口 : 80 查询

| 来源IP地址 | 通讯协议 | 来源端口 | 接口位置 | 目的IP地址 | 目的端口 | 下载带宽 Bytes/Sec | 上传带宽 Bytes/Sec |
|---|---|---|---|---|---|---|---|
| 60.248.180.226 | TCP | 2110 | WAN2 | 220.130.188.40 | 80 | 471 | 885 |
| 60.248.180.226 | TCP | 2111 | WAN2 | 220.130.188.40 | 80 | 52 | 57 |
| 60.248.180.226 | TCP | 2112 | WAN2 | 220.130.188.40 | 80 | 99 | 873 |
| 60.248.180.226 | TCP | 2113 | WAN2 | 220.130.188.40 | 80 | 52 | 57 |
| 60.248.180.226 | TCP | 2114 | WAN2 | 220.130.188.40 | 80 | 0 | 0 |

刷新





十五、注销

VPN 防火墙的网页窗口右上方有一个注销的按钮，此按钮为结束管理 VPN 防火墙并关闭此管理窗口。若您下次想再进入 VPN 防火墙管理窗口时，您必须重复登录 VPN 防火墙管理窗口的步骤，并输入管理者的使用名称与密码。








附录一、设置界面及使用手册章节对照

本章主要通过表格的形式把每个章节具体对照 VPN 防火墙 Web 管理页面的链接与界面对照显示，进一步方便用户快速的设置 VPN 防火墙，同时更加了解 VPN 防火墙的工作能力。

VPN 防火墙整体界面栏目次序图如下。




| 一级栏目 | 二级栏目 | 对应章节 |
|---|---|---|
| 首页 | | 五、确定设备规格、状态显示以及登录密码和时间的设置<br>5.1 首页显示 |
| 基本设置 | | 六、进行广域网络连线设置 |
| | 网络设置 | 6.1 网络设置 |
| | 流量管理 | 6.2 多 WAN 设置 |
| | 协议绑定 | 6.2 多 WAN 设置 |
| | 虚拟遶境 | 十一、虚拟绕径设置 |
| QoS 带宽管理 | | 八、QoS 带宽管理功能 |
| | 带宽管理 | 8.1 带宽设置(QoS)/ 8.3 智能带宽管理 |
| | 会话数管理 | 8.2 会话数管控 |
| IP/DHCP 设置 | | 七、内部局域网络设置 |





| | | |
|---|---|---|
| | DHCP 设置 | 7.3 DHCP 发放 IP 服务器 |
| | DHCP 状态 | 7.4 DHCP 状态显示 |
| | IP 与 MAC 绑定 | 7.5 IP 及 MAC 地址绑定 |
| | IP 群组管理 | 7.6 IP 群组管理 |
| 防火墙设置 | | 九、防火墙设置 |
| | 基本设置 | 9.1 基本设置/ 9.2 阻挡特定服务 |
| | 访问规则设置 | 9.3 访问规则设置 |
| | 内容过滤 | 9.4 网页内容管制 |
| 高级设置 | | 十二、其它进阶高级功能设置 |
| | DMZ/虚拟服务器 | 12.1 DMZ / 虚拟服务主机 |
| | UPnP 通讯协议 | 12.2 UPnP- Universal Plug and Play |
| | 路由通讯协议 | 12.3 路由通讯协议 |
| | 一对一 NAT | 12.4 一对一 NAT |
| | 动态域名服务 | 12.5 DDNS-动态域名解析 |
| | 广域网 MAC 地址设置 | 12.6 广域网接口 MAC 地址设置 |
| 系统工具 | | 十三、工具程序功能设置/五、确定设备规格、状态显示以及登录密码和时间的设置 |
| | 密码设置 | 5.2 登录密码和时间的设置 |
| | 自我诊断 | 13.1 在线联机测试 |
| | 软件更新 | 13.2 系统硬件升级 |
| | 设置参数备份/恢复 | 13.3 系统设置参数存储 |
| | SNMP 网路管理 | 13.4 网络管理设置(SNMP) |
| | 时间设置 | 5.2 登录密码和时间的设置 |
| | 系统恢复 | 13.5 系统恢复 |
| 端口管理 | | 七、内部局域网络设置 |
| | 端口设置 | 7.1 网络端口管理设置 |
| | 端口状态即时显示 | 7.2 网络端口状态实时显示 |
| VPN 虚拟专用网设置 | | 十、VPN 虚拟专用网 |
| | VPN 状态 | 10.1.1 目前所有 VPN 状态 |
| | 网关对网关设置 | 10.1.2.1 网关对网关设置 |
| | 客户端对网关设置 | 10.1.2.2 客户端对网关设置 |
| | PPTP 设置 | 10.1.3 PPTP 设置与状态 |
| | PPTP 状态 | 10.1.3 PPTP 设置与状态 |





| | | |
|---|---|---|
| | VPN 数据包穿透 | 10.1.4 VPN 数据包穿透防火墙功能 |
| QnoKey | | 10.2 QnoKey 设置 |
| | 设置与连接状态 | 10.2.1 -10.2.3 QnoKey 群组与用户设置 |
| QVM VPN | | 10.3 QVM VPN 功能设置 |
| | QVM 设置 | 10.3.1 QVM VPN 中心服务器端设置<br>10.3.3 QVM VPN 客户端设置 |
| | QVM 状态（服务器） | 10.3.2 QVM VPN 中央控管功能 |
| 日志 | | 十四、日志功能设置 |
| | 系统日志 | 14.1 系统日志 |
| | 系统状态 | 14.2 系统状态实时监控 |
| | 流量统计 | 14.3 流量统计 |
| | IP/端口流量监控 | 14.4 特定 IP 及端口状态 |





附录二：产品中有毒有害物质或元素表

| 部件名称 | 有毒有害物质或元素 | | | | | |
|---|---|---|---|---|---|---|
| | 铅(Pb) | 汞(Hg) | 镉(Cd) | 六价铬 (Cr(VI)) | 多溴联苯 (PBB) | 多溴二苯醚 (PBDE) |
| PCBA | X | O | O | O | O | O |

O：表示该有毒有害物质在部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。

X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 标准规定的限量要求。

- 电阻内部导通部位为导电银糊剂(含有铅玻璃料)
- Diode 本体有采用含有铅玻璃料





附录三：常见问题解决

（1） QQ 容易掉线问题

a). 检查 QQ 版本是否为 2006 版，经过 QQ 官方确认使用珊瑚版或是传美版掉线严重。

b). 2 条以上的线路，必须作协议绑定，让 QQ 走固定广域网。绑定 QQ(UDP8000~8004)走固定的广域网参照下图协议绑定设置：

**协议绑定**




c).保证带宽给 QQ 端口，依照网吧或企业内部实际带宽评估 QoS 所需要设置的最小值与最大值，下图为 10M 光纤保证给 QQ 的方式，上下传都必须设置。





## QoS带宽管理

控制类型： ⊙ 带宽控制 ○ 优先级

接口位置 : ☑ 广域网1 ☑ 广域网2 ☑ 广域网3 ☑ 广域网4

服务端口 : QQ [UDP/8000~8004]

服务端口新增或删除表

IP地址 : 0 . 0 . 0 . 0 到 0

目的 : 上传

保证带宽 : 200 Kbit/sec 最大可用带宽 : 2000 Kbit/sec

带宽分配方式 : ○ 此范围每一IP地址独享此设定带宽.
⊙ 此范围所有IP地址共享此设定带宽.

激活 : ☑

上移 | 更新特殊应用软件 | 下移

QQ [UDP/8000~8004]->0.0.0.0~0(上传)=>200~2000Kbit/sec->WAN1, 2, 3, 4

删除选中的项目 | 新增






（2）阻挡基本 BT 种子下载方式

若您想要封锁 BT 种子，不让用户下载，您可以直接在 "防火墙设置" => "内容过滤" 选择 "设定禁止访问的域名" 后将 "网页内容过滤(关键字)" 打入".torrent"这样就可以防止用户下载种子。

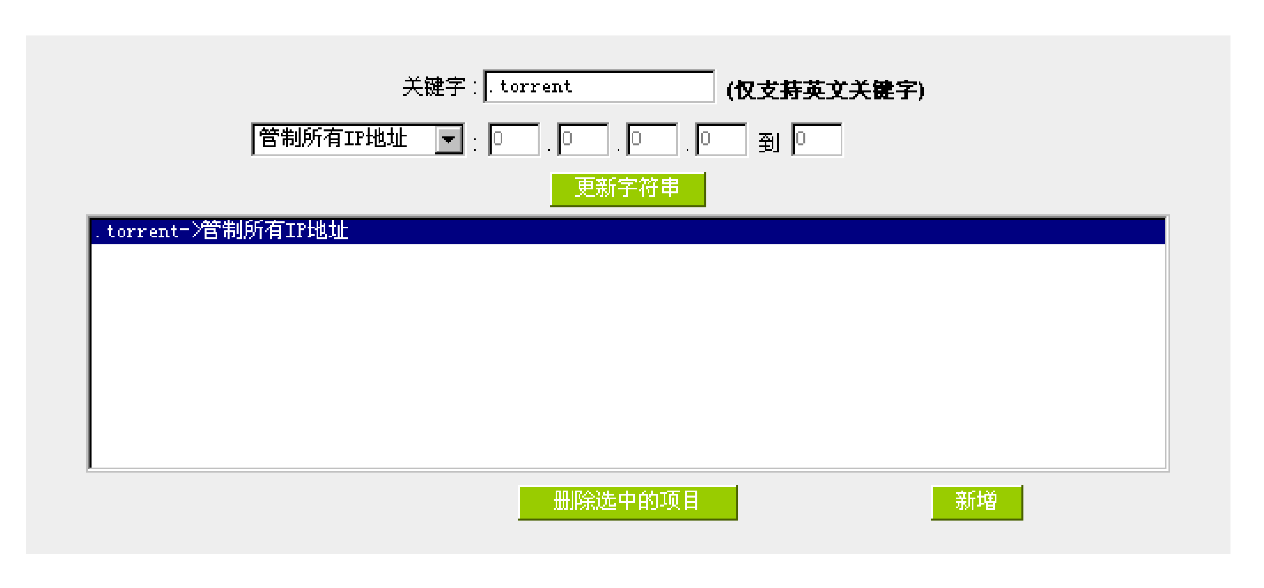
○ **设定允许访问的域名**
◉ **设定禁止访问的域名**

**禁止访问的域名**

☐ **激活**

**网页内容过滤(关键字)**

☑ **激活**



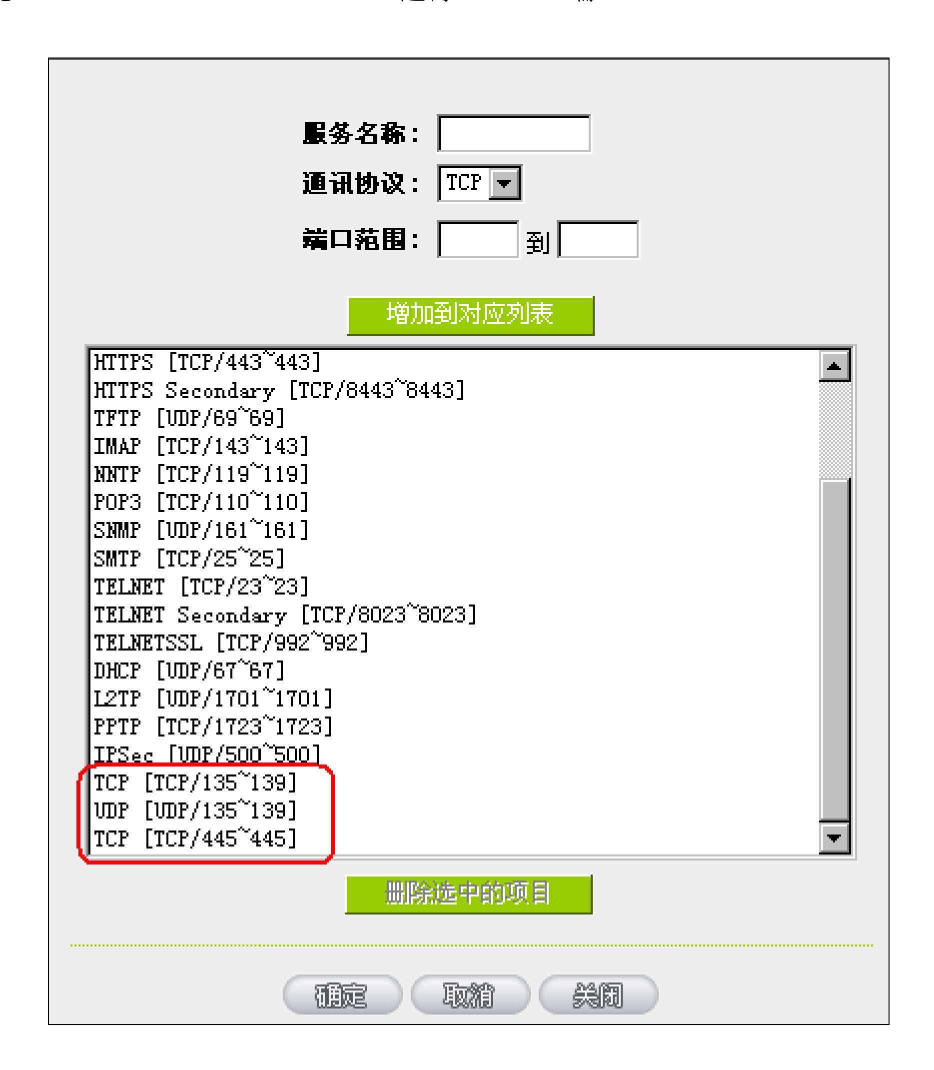




（3） 冲击波及蠕虫病毒的防制

由于近来还是发生有许多用户局域网中冲击波及蠕虫病毒造成局域网访问互联网很慢及联机数(Session)大量增加造成 VPN 防火墙大量处理，以下将指导您封锁此些病毒相应端口以达到防制目的。

a.增加此 TCP135-139， UDP135-139 还有 TCP445 端口:




b.用防火墙里面的"存取规则"功能将设置好的此三组端口封锁:






## 访问规则设置

| 管制动作： | 禁止 | |
|---|---|---|
| 服务端口： | TCP[TCP/135~139] | 服务端口新增或删除表 |
| 日志： | 激活 | |
| 接口位置： | 任何的 | |
| 来源IP地址： | 任何的 | |
| 目的IP地址： | 任何的 | |

用同样的方法添加好 UDP[UDP135~139]以及 TCP[445~445]端口。

c.将这三组的优先级至于最高：

跳到 1 / 2 页　　每页显示 5 笔　　下一页>>

| 优先级 | 激活 | 管制动作 | 服务端口 | 接口位置 | 来源IP地址 | 目的IP地址 | 管制时间 | 日 | 编辑 | 删除 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ☑ | 关闭 | TCP [445] | * | 任何的 | 任何的 | 所有时间 | | 编辑 | |
| 2 | ☑ | 关闭 | UDP [135] | * | 任何的 | 任何的 | 所有时间 | | 编辑 | |
| 3 | ☑ | 关闭 | TCP [135] | * | 任何的 | 任何的 | 所有时间 | | 编辑 | |
| | ☑ | 允许 | 所有端口 [*] | 局域网 | 任何的 | 任何的 | 所有时间 | | | |
| | ☑ | 关闭 | 所有端口 [*] | 广域网1 | 任何的 | 任何的 | 所有时间 | | | |

添加新规则　恢复出厂默认值





（4） 阻止 QQLive 视频直播设置

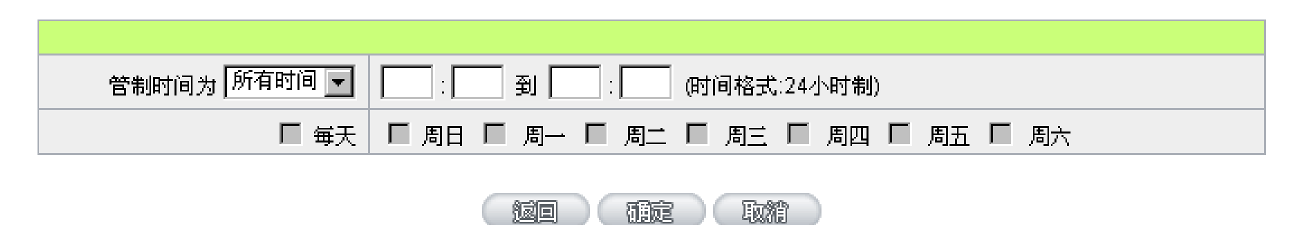
QQLive 视频直播软件是一种流媒体点播软件，最近好多客户都在头痛一个同样的问题，当局域网有多个用户使用 QQLive 视频直播软件，占用了比较大的带宽，造成 VPN 防火墙的负担过重，使得 VPN 防火墙反应迟钝或瘫痪，如果我们能够封锁 QQLive 的服务器登录过程就可以解决这样的问题，下面就这个问题来结合 Qno 产品的相关功能提出相关的解决方案，来进行 VPN 防火墙设置。

a). 进入 VPN 防火墙 Web 管理页面，再进入"防火墙设置"的"访问存取规则设置"。

## 访问规则设置

| | | |
|---|---|---|
| 管制动作： | 禁止 | |
| 服务端口： | 所有端口 [TCP&UDP/1~65535] | 服务端口新增或删除表 |
| 日志： | 关闭 | |
| 接口位置： | 任何的 | |
| 来源IP地址： | 任何的 | |
| 目的IP地址： | 单独 | 121 . 14 . 75 . 115 |

## 生效时间




b). 再点击"增加新的管制规则"，进入"访问存取规则设置"页面，在"存取服务规则设置"中的"管制动作"选项中选择"禁止"，再在"服务器端口" 选择"所有端口[TCP&UDP/1~65535]"，选择"来源接口"为"任何的"，"来源 IP 地址"选择"任何的"（有相关需求的用户可以选择"单独"或"范围" 阻止单个 IP 或者一段 IP 的 QQLive 的的登录）再在"目的 IP 地址"选择"单独"填入 QQLive 服务器的 IP 地址"121.14.75.115"（QQLive 服务器的 IP 地址不止一个，后面需要重复添加），最后在"时间管制设置"的"此存取规则选择" 所有时间"，"确定"后进入下一步骤。

c). 重复以上的操作在只替换"目的 IP 地址"里分别填入以下 IP 地址：

121.14.75.115

60.28.234.117





60.28.235.119

222.28.155.17

可封锁的 QQ Live 版本：QQ Live 2008 (7.0.4017.0)

测试日期:2008-07-29

重复添加后可以看到相关 QQLive 的服务器的连接被封锁，点击确认完成对阻止 QQLive 视频直播设置，此方案是在 QQLive3.1 的版本下测试并完成阻挡的。





（5） ARP 病毒攻击防制

1. ARP 问题的提出以及相关知识

近期，国内多家网吧出现短时间内断线(全断或部分断)的现象，但会在很短的时间内会自动恢复。这是因为 MAC 地址冲突引起的，当带毒机器的 MAC 映射到主机或者 VPN 防火墙之类的 NAT 设备，那么全网断线，如果只映射到网内其它机器，则只有这部分机器出问题。多发于传奇游戏特别是私服务外挂等方面。此类情况就是网络受到了 ARP 病毒攻击的明显表现，其目的在于，该病毒破解游戏加密解密算法，通过截取局域网中的数据包，然后分析游戏通讯协议的方法截获用户的信息。运行这个病毒，就可以获得整个局域网中游戏玩家的详细信息，盗取用户帐号信息。下面我们谈谈如何防制这种攻击。

首先，我们了解下什么是 ARP，ARP "Address Resolution Protocol"（地址解析协议），局域网中，网络中实际传输的是"帧"，帧里面是有目标主机 MAC 地址的。所谓"地址解析"就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

ARP 协议的工作原理：在每台安装有 TCP/IP 协议的计算机里都有一个 ARP 缓存表，表里的 IP 地址与 MAC 地址是一一对应的，如表所示。

| IP 址 | MAC 地址 |
|---|---|
| 192.168.1.1 | 00-0f-3d-83-74-28 |
| 192.168.1.2 | 00-aa-00-62-c5-03 |
| 192.168.1.3 | 03-aa-01-75-c3-06 |
| …… | …… |

我们以主机 A（192.168.1.5）向主机 B（192.168.1.1）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到相对应的 IP 地址，主机 A 就会在网络上发送一个广播，目标 MAC 地址是"FF.FF.FF.FF.FF.FF"，这表示向同一网段内的所有主机发出这样的询问："192.168.1.1 的 MAC 地址是什么？"网络上其它主机并不响应 ARP 询问，只有主机 B 接收到这个帧时，才向主机 A 做出这样的回应："192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09"。这样，主机 A 就知道了主机 B 的 MAC 地址，它就可以向主机 B 发送信息了。同时它还更新了自己的 ARP 缓存表。

再者，我们先简单介绍一下什么是 ARP 病毒攻击，这种病毒是对局域网的 PC 进行攻击，使局域网 PC 机的 ARP 表混乱，在局域网中，通过 ARP 协议来完成 IP 地址转换为第二层物理地址（即 MAC 地址）的。ARP 协议对网络安全具有重要的意义。通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP





通信量使网络阻塞。进行 ARP 复位向和嗅探攻击。用伪造源 MAC 地址发送 ARP 响应包，对 ARP 高速缓存机制的攻击。这些情况主要出现在网吧用户，造成网吧部分机器或全部机器暂时掉线或者不可以上网，在重新启动后可以解决，但保持不了多久有会出现这样的问题，网吧管理员对每台机器使用 arp –a 命令来检查 ARP 表的时候发现 VPN 防火墙的 IP 和 MAC 被修改，这就是 ARP 病毒攻击的典型症状。

这种病毒的程序如 PWSteal.lemir 或其变种，属于木马程序/蠕虫类病毒，Windows 95/98/Me/NT/2000/XP/2003 将受到影响，病毒攻击的方式对影响网络连接畅通来看有两种，对 VPN 防火墙的 ARP 表的欺骗和对局域网 PC 网关的欺骗，前者是先截获网关数据，再将一系列的错误的局域网 MAC 信息不停的发送给 VPN 防火墙，造成 VPN 防火墙发出的也是错误的 MAC 地址，造成正常 PC 无法收到信息。后者 ARP 攻击是伪造网关。它先建立一个假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的 VPN 防火墙途径上网。在 PC 看来，就是上不了网了，"网络掉线了"。

就这两种情况而言，如果对 ARP 病毒攻击进行防制的话我们必须得做 VPN 防火墙方面和客户端双方的设置才保证问题的最终解决。所以我们选择 VPN 防火墙的话最好看看 VPN 防火墙是否带有防制 ARP 病毒攻击的功能，Qno 产品正好提供了这样的功能，相比其它产品操作简单易学。

2. ARP 的判断

如过网络中有一台或多台计算机受到或已经感染了 ARP 病毒，我们就必须学会判断并采取相应的解决方法处理类似问题的发生，下面来谈谈 Qno 技术工程师的 ARP 防制经验谈。

通过对 ARP 工作原理得知，如果系统 ARP 缓存表被修改不停的通知 VPN 防火墙一系列错误的局域网 IP 或者干脆伪造一个假的网关进行欺骗的话，网络就肯定会出现大面积的掉线问题，这样的情况就是典型的 ARP 攻击，对遭受 ARP 攻击的判断，其方法很容易，你找到出现问题的计算机点开始运行进入系统的 DOS 操作。pingVPN 防火墙的 LAN IP 丢包情况。输入 ping 192.168.1.1（网关 IP 地址），如图。

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

局域网 pingVPN 防火墙的 LAN IP 丢几个包，然后又连上，这很有可能是中了 ARP 攻击。为了进一步确认，我们可以通过查找 ARP 表来判断。输入 ARP -a 命令，显示如下图。





```
Interface: 192.168.1.72 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0f-3d-83-74-28     dynamic
  192.168.1.43          00-13-d3-ef-b2-0c     dynamic
  192.168.1.252         00-0f-3d-83-74-28     dynamic

C:\WINDOWS\System32>arp -a
```

可以看出 192.168.1.1 地址和 192.168.1.252 地址的 IP 的 MAC 地址都是 00-0f-3d-83-74-28，很显然，这就是 ARP 欺骗造成的。

3. ARP 的解决

我们现在已经理解了 ARP，ARP 欺骗攻击以及如何判断此类攻击，下面的问题就是如何找到行之有效的防制办法来防止这类攻击对网络造成的危害。Qno 的一般处理办法分三个步骤来完成。

a）、激活防止 ARP 病毒攻击：

输入 VPN 防火墙 IP 地址，登陆 VPN 防火墙的 Web 管理页面，进入"防火墙设置"的"基本设置"，再在右边找到"防止 ARP 病毒攻击"在这一行的"激活"前面做点选，再在页面最下点击"确认"，如图。

| | |
|---|---|
| 防火墙： | ⦿ 激活 ○ 关闭 |
| SPI数据包检测： | ⦿ 激活 ○ 关闭 |
| 防止DoS攻击功能： | ⦿ 激活 ○ 关闭 高级设定 |
| 阻止广域网回应功能： | ○ 激活 ⦿ 关闭 |
| 远程管理功能： | ⦿ 激活 ○ 关闭 端口：80 |
| 允许Multicast组播穿透： | ○ 激活 ⦿ 关闭 |
| 防止ARP病毒攻击： | ⦿ 激活 ○ 关闭<br>每秒主动发送 20 笔ARP封包 |

b）、在每台 PC 上绑定网关的 IP 和其 MAC 地址

进行这样的操作主要防止 ARP 欺骗网关 IP 和其 MAC 地址首先在 VPN 防火墙端查找网关 IP 与 MAC 地址，如图。





### 局域网(LAN)接口配置

| | |
|---|---|
| MAC地址： | 00 - 17 - 16 - 01 - 35 - cf<br>(默认值: 00-17-16-01-35-cf) |
| 局域网网关： | 192 . 168 . 1 . 1 |
| 子网掩码： | 255 . 255 . 255 . 0 |

然后在每台 PC 机上开始/运行 cmd 进入 dos 操作，输入 arp –s 192.168.1.1 00-17-16-01-35-cf，Enter 后完成 pc01 的绑定。如图

```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>arp -s 192.168.1.1 00-17-16-01-35-cf
```

针对网络内的其它主机用同样的方法输入相应的主机 IP 以及 MAC 地址完成 IP 与 MAC 绑定。但是此动作，如果重起了计算机，作用就会消失，所以可以把此命令做成一个批处理文件，放在操作系统的启动里面，批处理文件可以这样写：

@echo off

arp -d

arp -sVPN 防火墙 LAN IP　VPN 防火墙 LAN MAC

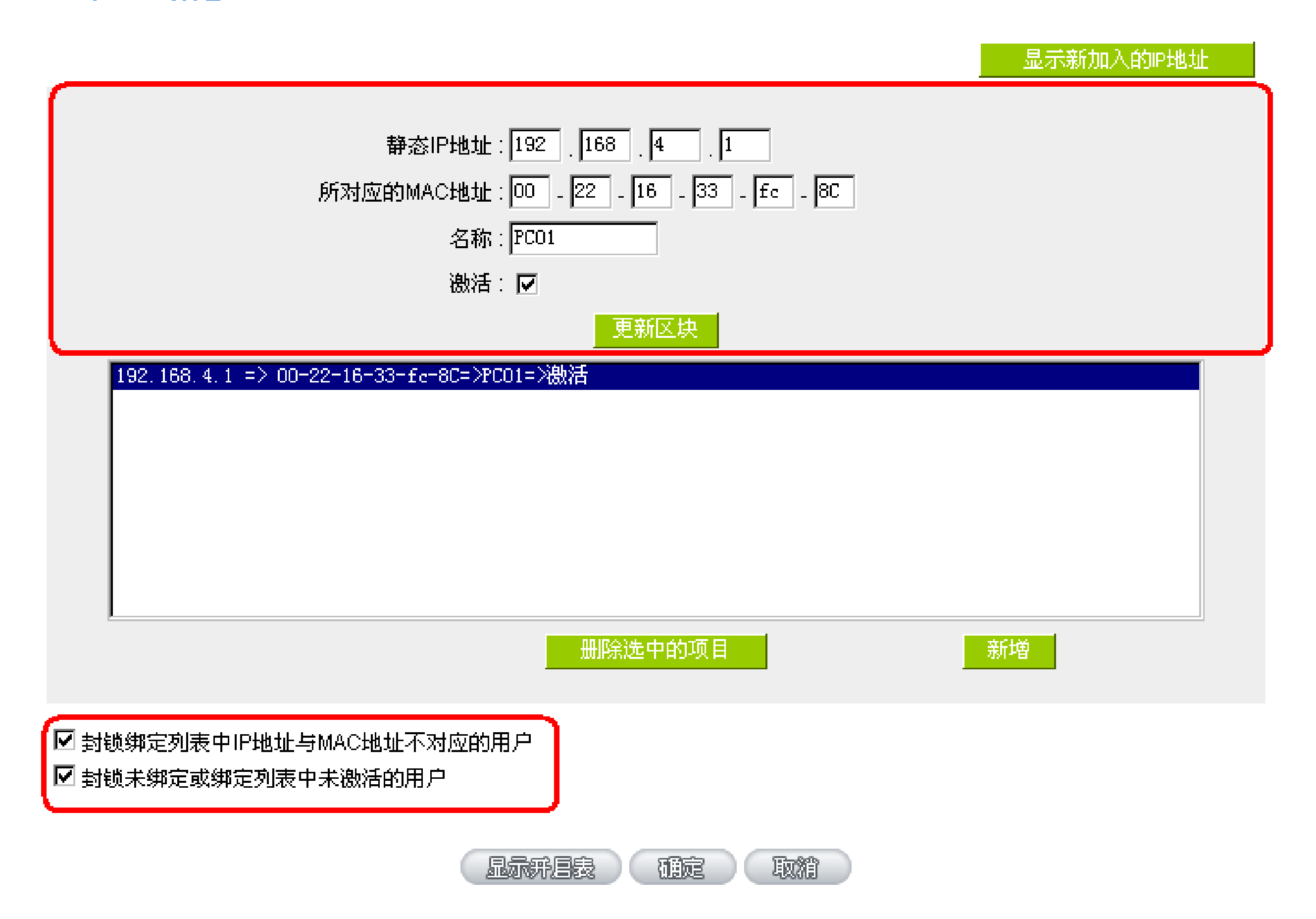
对于已经中了 arp 攻击的局域网，要找到攻击源。方法：在 PC 上不了网或者 ping 丢包的时候，在 DOS 下打 arp –a 命令，看显示的网关的 MAC 地址是否和 VPN 防火墙真实的 MAC 相同。如果不是，则查找这个 MAC 地址所对应的 PC，这台 PC 就是攻击源。

其它的 VPN 防火墙用户的解决方案也是要在 VPN 防火墙和 PC 机端进行双向绑定 IP 地址与 MAC 地址来完成相应防制工作的，但在 VPN 防火墙端和 PC 端对 IP 地址与 MAC 地址的绑定比较复杂，需要查找每台 PC 机的 IP 地址与 MAC 加大了工作量，操作过程中还容易出错。

c)、在 VPN 防火墙端绑定用户 IP/MAC 地址：

进入"IP / DHCP 设置功能"，可以看到"IP 与 MAC 绑定"，你可以在此添加 IP 与 MAC 绑定，输入相关参数，在"激活"上点 "√" 选再"添加到对应列表"，重复操作添加局域网里的其它 IP 与 MAC 的绑定，再点页面最下的"确定"。

## IP与MAC绑定




当添加了对应列表之后，其对应的信息就会在下面的白色框里显示出来。不过建议不采用此方法，这样操作需要查询网络内所有主机 IP/MAC 地址工作量繁重，还有一种方法来绑定 IP 与 MAC，操作会相对容易，可以减少大量的工作量，节约大量时间，下面就会讲到。

进入"IP / DHCP 设置"的"IP 与 MAC 绑定"右边有一个"显示新加入的 IP 地址"点击进入。





显示新加入的IP地址

静态IP地址：. . .
所对应的MAC地址：- - - - -
名称：
激活：
增加到对应列表

删除选中的项目

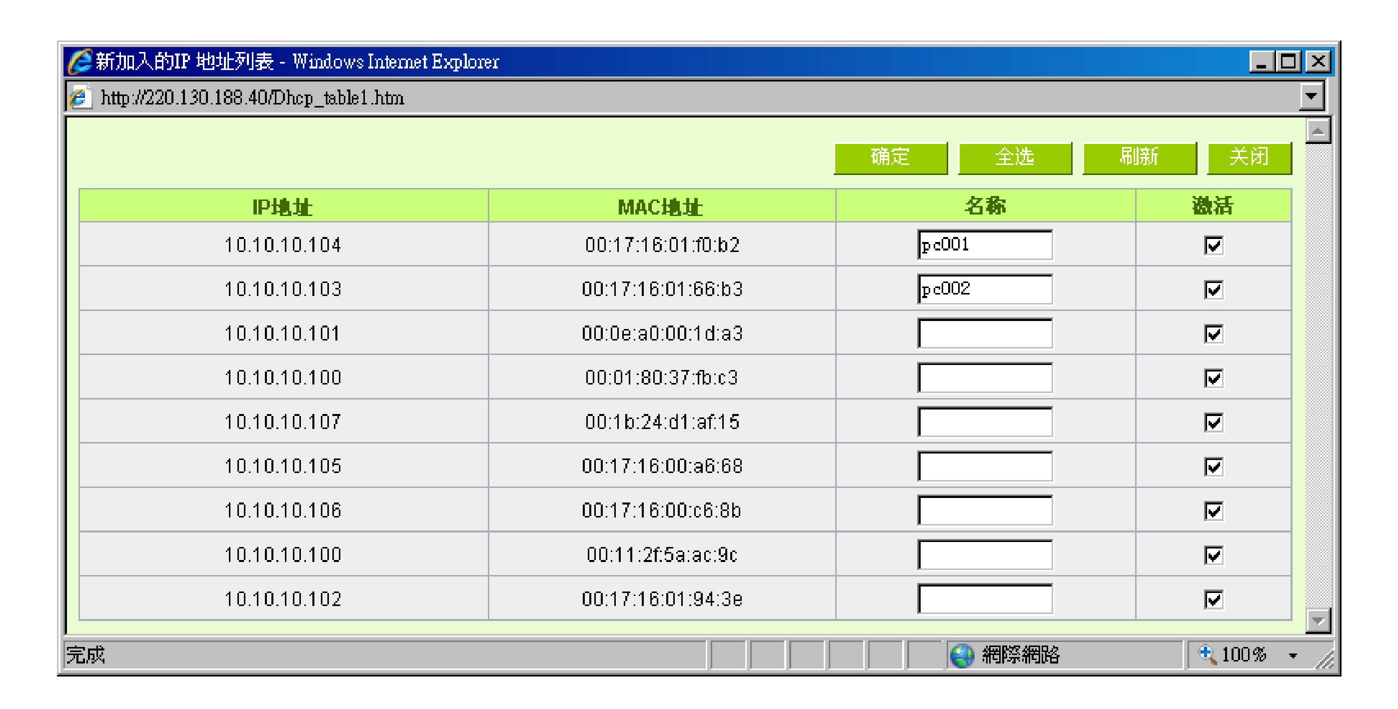
封锁绑定列表中IP地址与MAC地址不对应的用户
封锁未绑定或绑定列表中未激活的用户

显示开启表 确定 取消

点击之后会弹出 IP 与 MAC 绑定列表对话框，此对话框里会显示网内未做绑定的 pc 的 IP 与 MAC 地址对应情况，输入计算机"名称"和"激活"上 "√" 选，再在右上角点确定。



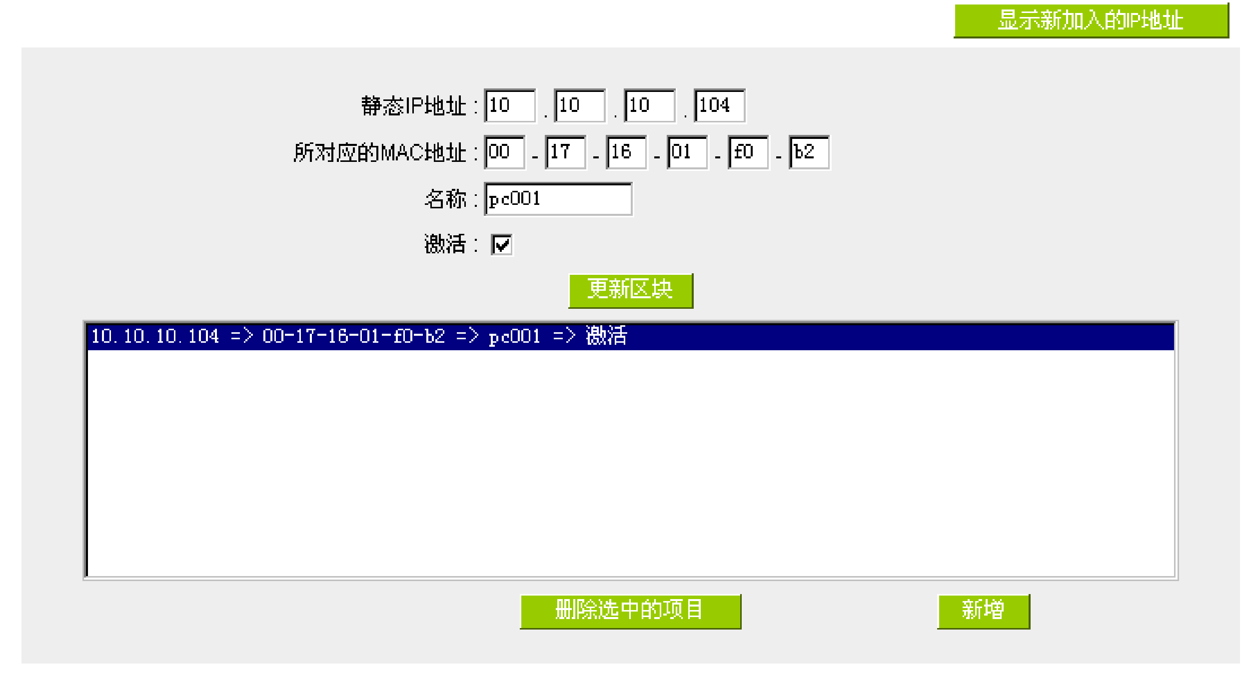





| IP地址 | MAC地址 | 名称 | 激活 |
| --- | --- | --- | --- |
| 10.10.10.104 | 00:17:16:01:f0:b2 | pc001 | ☑ |
| 10.10.10.103 | 00:17:16:01:66:b3 | pc002 | ☑ |
| 10.10.10.101 | 00:0e:a0:00:1d:a3 | | ☑ |
| 10.10.10.100 | 00:01:80:37:fb:c3 | | ☑ |
| 10.10.10.107 | 00:1b:24:d1:af:15 | | ☑ |
| 10.10.10.105 | 00:17:16:00:a6:68 | | ☑ |
| 10.10.10.106 | 00:17:16:00:c6:8b | | ☑ |
| 10.10.10.100 | 00:11:2f:5a:ac:9c | | ☑ |
| 10.10.10.102 | 00:17:16:01:94:3e | | ☑ |

此时你所绑定的选项就会出现在 IP 与 MAC 绑定列表框里，如图 5 再点击"确认"绑定完成。

## IP与MAC绑定




即便我们单靠这样的操作基本可以解决问题，但 Qno 的技术工程师建议通过进一步通过一些手段来进一步控制 ARP 的攻击。

1、病毒源，对病毒源头的机器进行处理，杀毒或重新装系统。此操作比较重要，解决了 ARP 攻击的源头 PC 机的问题，可以保证局域网免受攻击。

2、网吧管理员检查局域网病毒，安装杀毒软件（金山毒霸/瑞星，必须要更新病毒代码），对机器进行病毒扫描。

3、给系统安装补丁程序。通过 Windows Update 安装好系统补丁程序(关键更新、安全更新和 Service Pack)

4、给系统管理员帐户设置足够复杂的强密码，最好能是 12 位以上，字母+数字+符号的组合；也可以禁用/删除一些不使用的帐户

5、经常更新杀毒软件（病毒库），设置允许的可设置为每天定时自动更新。安装并使用网络防火墙软件，网络防火墙在防病毒过程中也可以起到至关重要的作用，能有效地阻挡自来网络的攻击和病毒的入侵。部分盗

版 Windows 用户不能正常安装补丁，不妨通过使用网络防火墙等其它方法来做到一定的防护

6、关闭一些不需要的服务，条件允许的可关闭一些没有必要的共享，也包括 C$、D$等管理共享。完全单机的用户也可直接关闭 Server 服务

7、不要随便点击打开 QQ、MSN 等聊天工具上发来的链接信息，不要随便打开或运行陌生、可疑文件和程序，如邮件中的陌生附件，外挂程序等。

4. 总结

ARP 攻击防制是一个任重而道远的过程，以上方法基本可以解决 ARP 病毒攻击对网络造成相关问题，而且客户采取类似的方法也收到了很大的效果，但还是提醒网落管理人员必须高度重视这个问题，而且不能大意马虎，我们可以采取以上建议随时警惕 ARP 攻击，以减少受到的危害，提高工作效率，降低经济损失。





附录四：Qno 技术支持资讯

更多有关侠诺产品技术资讯，除了可以登录侠诺宽带讨论区、参照 FTP 服务器的相关实例；或是进一步联系侠诺各经销商技术部门、或侠诺大陆技术中心取得相关协助。

网上讨论区及 FTP 服务器：

讨论区：http://www.Qno.cn/forum

各大经销商服务联系方式：

用户可以登录网站先上服务页面查询各大经销联系方法：

http://www.Qno.cn/web/where_buy.asp

技术中心：

电邮：QnoFAE@qno.com.tw